Center2
取扱説明書

NetSpring®

株式会社ネットスプリング

2012年1月

はじめに

　このたびは Center2 をお買い上げ頂き、誠にありがとうございます。
正しく安全にお使い頂くため、ご使用前に必ず本書をお読みください。
本書は、Center2 Ver 2.1.3 を対象にしています。

安全上の注意

　次の表示区分は、表示内容を守らず、誤った使用をした場合に生じる危険や損害の程度を説明しています。

	警告	この表示は、誤った使用をした場合、「人が死亡または重傷を負う可能性が想定される」内容を示しています。
	注意	この表示は、誤った使用をした場合、「人が障害を負う可能性または物的損害が発生する可能性が想定される」内容を示しています。

　次の表示区分は、お守りいただく内容を説明しています。

	禁止（してはいけないこと）を示しています。
	強制（必ず実行していただくこと）を示しています。

	警告	
	同梱の電源ケーブル以外は、使用しないでください。	故障したり、過熱、発煙するおそれがあり、火災、感電の原因となります。
	強い衝撃を与えたり、投げつけたりしないでください。	故障したり、過熱、発煙するおそれがあり、火災、感電の原因となります。

	分解、改造をしないでください。	火災、感電、ケガなどの事故または故障の原因となります。
	水につけたり、ぬらしたりしないでください。	故障したり、過熱、発煙するおそれがあり、火災、感電の原因となります。
	ぬれた手で本製品やプラグを触らないでください。	火災、感電、ケガなどの事故または故障の原因となります。
	本製品に水や殺虫剤などをかけたりしないでください。	故障したり、過熱、発煙するおそれがあり、火災、感電の原因となります。
	端子部を触らないでください。	故障したり、感電、ケガのおそれがあります。
	通気孔をふさがないでください。	故障したり、過熱、発煙するおそれがあり、火災、感電の原因となります。
	通気孔に物を差し込まないでください。	故障したり、過熱、発煙するおそれがあり、火災、感電の原因となります。
	本体が異常に熱くなったり、煙が出たり、変なにおいがした場合は、電源プラグをコンセントから抜いて弊社サポートセンターへご連絡ください。	火災の原因となります。

	注意	
	本書に記載されていない操作はしないでください。	故障の原因となります。
	動作中に本体を長時間触らないでください。	低温やけどを負う可能性があります。

諸注意

- 本製品は「外国為替および外国貿易管理法」に定められる戦略物資等に該当します。本製品を輸出または日本国外へ持ち出す際には、事前に弊社の書面による承諾を得ることのほか、同法および関連の法令に基づく手続きが必要です。
- 本製品は日本国内仕様のため、修理・保守サービス・技術サポートなどの対応は、日本国外ではお受けできませんのでご了承ください。
- 日本国外ではその国の法律または規制により、本製品を使用できないことがあります。このような国では、本製品を使用した結果罰せられることがありますが、弊社は一切の責任を負いかねますのでご了承ください。

商標

- FEREC は株式会社ネットスプリングの登録商標です。
- 本書に記載されている他社製品名は、一般に各社の商標または登録商標です。

本書について

- 本書の著作権は株式会社ネットスプリングに帰属します。本書の一部または全部を無断で転載、複製、改変などを行うことは禁じられています。
- 本書の校正には細心の注意を払っておりますが、技術的な誤りまたは誤植のある可能性があります。お気付きの点がございましたら、弊社までご連絡ください。
- 本書に記載された内容は、予告なく改良または変更する場合があります。

改訂番号	5
改訂日	2012 年 1 月 26 日

目次

1. お使いいただく前に

1.1. 製品の特徴

FERECを集中管理

最大50台までのFEREC520/720を効率よく集中管理できます。

ログを一括管理

FERECのログを収集・保存し、一括して管理できます。

FERECを一括設定

FERECの各種設定を一括してできます。

ユーザ利用状況

ユーザ利用状況をリアルタイム表示できます。

ユーザ利用履歴を一括管理

ユーザのログイン履歴を収集・保存し、一括して管理できます。

簡単な設定･運用管理

ウェブブラウザによる簡易な設定、運用管理ができます。

最新ファームウェアを提供

最新ファームウェアはFERECオフィシャルサイト（http://www.ferec.jp/）からダウンロードできます。

1.2. 本体各部の名称

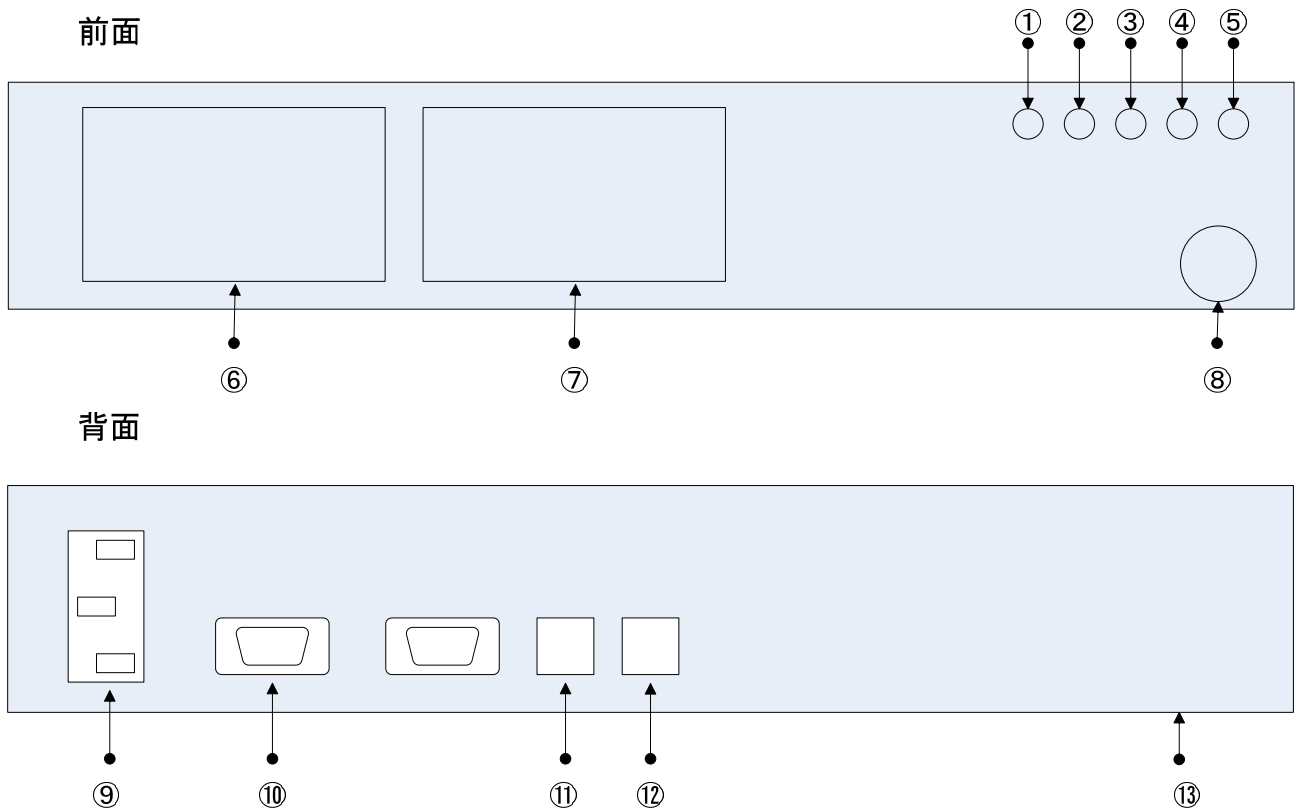
Center2 各部の名称と機能は以下のとおりです。

前面

①　②　③　④　⑤

⑥　⑦　⑧

背面

⑨　⑩　⑪　⑫　⑬

① オーバーヒート LED

オーバーヒート状態の時、点滅します。点滅している場合は、設置場所の室内温度等に問題ないかご確認下さい。

② MNT ポート LED

③ LAN ポート LED

MNT、LAN ポートがリンクアップすれば点灯します。また、アクセスがあれば点滅します。

④ HDD LED

HDD アクセスがあれば点滅します。

⑤ POWER LED

電源がオンの時、点灯します。

⑥　ドライブ１

⑦　ドライブ２

データディスクです。Center2 を起動する際は、必ず接続してください。

⑧　電源スイッチ

電源スイッチです。電源がオフの時に押すと電源が入ります。

⑨　AC 入力

電源コネクタです。必ず付属の電源ケーブルを接続してください。

⑩　CONSOLE ポート

シリアルコンソール用の RS-232C ポートです。管理用 PC と接続する際はクロスケーブルを使用します。

⑪　LAN ポート

⑫　MNT ポート

LAN、MNT 用のイーサネットポートです。

FDJ400 の場合

ポート右上の LED は、リンクアップすれば橙色に点灯し、アクセスがあれば点滅します。

ポート左上の LED は、1000Mbps でリンクアップした場合は橙色に、100Mbps および 10Mbps でリンクアップした場合は消灯します。

FDJ401 および FDJ402 の場合

ポート右上の LED は、リンクアップすれば黄色に点灯し、アクセスがあれば点滅します。

ポート左上の LED は、1000Mbps でリンクアップした場合は橙色に、100Mbps でリンクアップした場合は黄緑色に点灯し、10Mbps でリンクアップした場合は消灯します。

⑬　シリアル番号

シリアル番号を記載しています。本体斜め上からご確認下さい。

注）ここに記載していないコネクタには何も接続しないでください。もし接続された場合には、故障の原因になる場合があります。

1.3. 起動・停止

Center2 の起動は、本体前面の電源スイッチを押します。1 分程度で使用可能な状態となり、本体から「ぽぴっ」という音がします。

起動中、電源スイッチを押すと停止します。また、停止は、ウェブブラウザで管理ページにアクセスし、[Center2 管理] → [停止] 画面から行うこと、コマンドラインで “halt” コマンドで行うこともできます。

これら以外の方法で、電源断しますと Center2 本体内にある FEREC ログなどのデータの一部あるいは全部が破損する恐れがあります。

2. Center2 の管理方法

Center2 の設定および管理は、ウェブブラウザで行う方法と telnet や ssh を用いてコマンドラインで行う方法の 2 通りがあります。

2.1. ウェブブラウザで設定および管理を行う

ウェブブラウザで設定および管理をするには以下の 2 つの方法があります。

2.1.1. MNT ポートに接続する場合

① PC の LAN ポートと Center2 の MNT ポートをクロス結線の LAN ケーブルで直接接続します。

② PC のネットワーク設定は DHCP クライアントとして設定を行います。

③ PC は DHCP サーバからの IP アドレス割り当てに失敗し、自動的に PC には 169.254.***.***という IP アドレスが割り当てられます。この際、IP アドレスが割り当てられるまで約 1 分程度かかります。

④ PC でウェブブラウザを起動し、"http://169.254.35.3:800/"を入力してページを開きます。

⑤ Center2 管理ページを開くためのユーザ名とパスワード入力画面が表示されますので、ユーザ名欄には admin、パスワード欄には設定してあるパスワードを入力します。工場出荷時のパスワードは admin です。

NOTE

- もしパスワードが不明になった場合は、ユーザ名 mntadmin、パスワード cu$U2xjQ を入力すると Center2 管理ページを開くことができます。
- HTTPS 設定の設定内容に関わらず、MNT ポートは常に HTTP のみでアクセス可能です。
- 管理許可アドレス設定の設定内容に関わらず、MNT ポートは常に接続できます。

2.1.2. LAN ポート経由で接続する場合

① PC と Center2 をネットワークを経由して接続します。もし PC と Center2 を直接 LAN ケーブルで接続する場合は、PC の LAN ポートと Center2 の LAN ポートをクロス結線の LAN ケーブルで接続します。

② PC はネットワーク環境に応じてネットワーク設定を行います。

③ PC でウェブブラウザを起動し、“http://［Center2 の IP アドレス］:800/” を入力してページを開きます。但し、HTTPS を使用する設定の場合は、“https://［Center2 の IP アドレス］:800/” を入力します。

④ Center2 管理ページを開くためのユーザ名とパスワード入力画面が表示されますので、ユーザ名欄には admin、パスワード欄には設定してあるパスワードを入力します。工場出荷時のパスワードは admin です。

NOTE

- 工場出荷時、Center2 の IP アドレスは、192.168.45.1 です。PC と Center2 を直接 LAN ケーブルで接続する場合、PC のネットワーク設定で 192.168.45.2 などの IP アドレスを設定しておく必要があります。

2.2. コマンドラインで設定および管理を行う

コマンドラインで設定および管理をするには以下の 3 つの方法があります。

NOTE

- 日本語の入力および表示を行う必要がある設定についてはコマンドラインではなくウェブブラウザを使用して設定を行ってください。コマンドラインでは日本語の入力は行えません。

2.2.1. MNT ポートに接続する場合

① PC の LAN ポートと Center2 の MNT ポートをクロス結線の LAN ケーブルで直接接続します。

② PC のネットワーク設定は DHCP クライアントとして設定を行います。

③ PC は DHCP サーバからの IP アドレス割り当てに失敗し、自動的に PC には 169.254.***.***という IP アドレスが割り当てられます。この際、IP アドレスが割り当てられるまで約 1 分程度かかります。

④ PC で telnet クライアントソフトを起動し、“169.254.35.3”に接続します。

⑤ Center2 管理コンソールへログインするためのログインプロンプトが表示されますので、login:プロンプトには admin、Password:プロンプトには設定してあるパスワードを入力します。工場出荷時のパスワードは admin です。

NOTE

- もしパスワードが不明になった場合は、ユーザ名 mntadmin、パスワード cu$U2xjQ を入力すると Center2 管理コンソールへログインすることができます。
- admin sshd コマンド、admin telnetd コマンドの設定内容に関わらず、MNT ポートは常に telnet のみでアクセス可能です。
- 管理許可アドレス設定の設定内容に関わらず、MNT ポートは常に接続できます。

2.2.2. LAN ポート経由で接続する場合

① PC と Center2 をネットワークを経由して接続します。もし PC と Center2 を直接 LAN ケーブルで接続する場合は、PC の LAN ポートと Center2 の LAN ポートをクロス結線の LAN ケーブルで接続します。

② PC はネットワーク環境に応じてネットワーク設定を行います。

③ PC で telnet クライアントソフトを起動し、Center2 の IP アドレスに接続します。

④ Center2 管理コンソールにログインするためのログインプロンプトが表示されますので、login:プロンプトには admin、Password:プロンプトには設定してあるパスワードを入力します。工場出荷時のパスワードは admin です。

NOTE

- 工場出荷時、Center2 の IP アドレスは 192.168.45.1 です。PC と Center2 を直接 LAN ケーブルで接続する場合、PC のネットワーク設定で 192.168.45.2 などの IP アドレスを設定しておく必要があります。
- Center2 の設定で、管理コンソールへの接続に SSH を許可している場合は PC で SSHv2 クライアントソフトを起動し、Center2 の IP アドレスに接続して、Center2 管理コンソールを利用することができます。

SSHv2 を使用するには、Center2 管理コンソールから以下のコマンドを実行します。

```
> admin sshd enable
```

2.2.3. CONSOLE ポートに接続する場合

① PC のシリアルポートと Center2 の CONSOLE ポートをクロス（リバース）結線の RS-232C ケーブルで接続します。

② PC でターミナルエミュレータソフトを起動し、以下の設定で接続します。

項目	設定値
ボーレート	9600bps
データ長	8bit
パリティ	なし
ストップビット	1
フロー制御	なし

③ Center2 管理コンソールへログインするためのログインプロンプトが表示されますので、login:プロンプトには admin を、Password:プロンプトには設定してあるパスワードを入力します。工場出荷時のパスワードは admin です。

NOTE

- もしパスワードが不明になった場合は、ユーザ名 mntadmin、パスワード cu$U2xjQ を入力すると Center2 管理コンソールへログインすることができます。

2.3. 管理ページへのアクセス制限

Center2 では、管理ページおよび管理コンソール（telnet,ssh）へのアクセスを、許可した特定のアドレスのみに制限することができます。設定方法は、“8.2.1. 管理許可アドレス設定”を参照してください。

3. 基本設定

Center2 は、次の 3 つの設定を行っていただければ、簡単にご利用を開始いただけます。

ステップ 1	Center2 の IP アドレスを設定する
ステップ 2	管理する FEREC を登録する
ステップ 3	管理する FEREC に Center2 を登録する

この他にも Center2 をより良くご利用いただくための設定があります。詳しくは、次章以降をご参照下さい。

3.1. Center2 の IP アドレスを設定する

お客様のご利用環境に合わせて、Center2 の IP アドレスを設定下さい。

登録は、ウェブブラウザから、または、コマンドラインで行います。詳しくは、“2. Center2 の管理方法”をご参照下さい。

ウェブブラウザで行う場合

［Center2 設定］→［ネットワーク］→［アドレス設定］画面で行います。

コマンドラインから行う場合

“**network address**”コマンドを使用します。

```
> network address 192.168.100.50/24
```

3.2. 管理する FEREC を登録する

Center2 で管理する各 FEREC の IP アドレスをご登録下さい。

登録は、ウェブブラウザから、または、コマンドラインで行います。

ウェブブラウザで行う場合

［FEREC 管理］→［管理対象一覧］→［追加］画面で行います。

コマンドラインから行う場合

“**node add**”コマンドを使用します。

```
> node add 3 192.168.130.10 2 ”Second Floor”
```

3.3. 管理する FEREC に Center2 を登録する

管理する各 FEREC で個々に Center2 の IP アドレスをご登録下さい。

登録は、ウェブブラウザから、または、コマンドラインで行います。なお、詳しい登録方法は「FEREC520/720 取扱説明書」をご参照下さい。

ウェブブラウザで行う場合

管理用 PC でウェブブラウザを起動し、FEREC 管理ページにログイン後、[設定] → [システム設定] → [Center2 設定] 画面で行います。

コマンドラインから行う場合

管理用 PC で telnet クライアントを起動し、FEREC に直接ログイン後、“**admin center2 add**” コマンドを使用します。

```
> admin center2 add 192.168.100.50
```

4. 管理ページ

ウェブブラウザでアクセスすると、最初に以下のような Center2 の画面（以降、Center2 管理ページと呼びます）が表示されます。

FEREC Center2
③ バージョン: Center2-2.1
Center2 管理ページ
①
▼ Top
▸ FEREC 設定
▸ FEREC 状態表示
▸ FEREC 管理
▸ Center2 設定
▸ Center2 状態表示
▸ Center2 管理
② FEREC の台数 (稼働中/登録台数) 2/2

① 各管理機能のメニュー
② 管理対象として登録されている FEREC の台数と、その中で稼働中の台数を表示
③ Center2 のファームウェアバージョン

Center2 管理ページは、以下のような構成になっています。

- FEREC設定
  - ネットワーク
    - DNS一括設定
  - アクセスコントロール
    - FTPプロキシ一括設定
  - 認証
    - 優先順位一括設定
    - RADIUS認証一括設定
    - LDAP認証一括設定
    - 内部認証一括設定
    - 禁止アカウント一括設定
  - クライアント設定
    - HTTP外部プロキシ一括設定
      - プロキシサーバ一括設定
    - 重複ログイン一括設定
    - ポーリング間隔一括設定
    - 利用時間帯制限一括設定
  - 認証ページ設定
    - ロゴ表示一括設定
    - メッセージカタログ一括設定
    - アクション一括設定

4. 管理ページ

- FEREC設定
  - システム設定
    - 管理許可アドレス一括設定
    - RADIUSアカウンティング一括設定
    - syslog一括設定
    - 時刻一括設定
    - 管理者パスワード一括設定
    - FTPパスワード一括設定
  - 設定のコピー
- FEREC状態表示
  - FEREC状態一覧
  - ログインユーザー覧
  - FERECログ
  - FERECログイン履歴
- FEREC管理
  - 管理対象一覧
  - グループ一覧
  - 一括設定初期化
  - 一括再起動
  - 一括ステータスダンプ取得
  - 一括バックアップ取得
  - 一括ファームウェア更新

- Center2設定
  - ネットワーク
    - アドレス設定
    - DNS設定
  - システム設定
    - 管理許可アドレス設定
    - HTTPS設定
      - 証明書インポート
      - 証明書エクスポート
    - syslog設定
    - 時刻設定
- Center2状態表示
  - ログ
  - 設定一覧
  - 本体情報
- Center2管理
  - ディスク管理
  - パスワード
  - 初期化
  - 再起動
  - 停止
  - ステータスダンプ
  - バックアップ
  - ファームウェア更新
  - ping

5. FEREC 設定

FEREC 設定には、以下の機能があります。

機能	概要
ネットワーク	グループ単位で FEREC のネットワーク関連の設定を行います。
アクセスコントロール	グループ単位で FEREC のアクセスコントロールの設定を行います。
認証	グループ単位で FEREC の内部認証の管理、および外部認証の設定を行います。
クライアント設定	グループ単位で FEREC のクライアントに関する設定を行います。
認証ページ設定	グループ単位で FEREC の認証ページのカスタマイズを行います。
システム設定	グループ単位で FEREC の上記以外のシステム設定を行います。
設定のコピー	グループ単位で指定した FEREC の設定の一部をコピーします。

5.1.　ネットワーク

ネットワークには、以下の機能があります。

機能	概要
DNS 一括設定	グループ単位で DNS の設定を行います。

5.1.1. DNS 一括設定

DNS 一括設定では、グループ登録した FEREC に一括して DNS サーバを設定することができます。

- **手順 1: ［DNS 一括設定］画面を開く**

  Center2 管理ページより［FEREC 設定］→［ネットワーク］→［DNS 一括設定］画面を開きます。

- **手順 2: グループの選択**

  ［グループ］のプルダウンメニューから、DNS サーバを設定するグループを選択します。

- **手順 3: 設定対象の選択**

  ［設定対象］のプルダウンメニューから、設定対象を選択します。

- **手順 4: IP アドレスの設定**

  ［IP アドレス］欄に DNS サーバの IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

- **手順 5: 設定**

  ［設定］ボタンを押すと、グループに属する全 FEREC に指定した DNS サーバが設定されます。

5.2. アクセスコントロール

アクセスコントロールには、以下の機能があります。

機能	概要
FTP プロキシ一括設定	グループ単位で FTP プロキシの設定を行います。

FEREC Center2
バージョン: Center2-2.1

Top
FEREC 設定
ネットワーク
アクセスコントロール
FTPプロキシ一括設定
認証
クライアント設定
認証ページ設定
システム設定
設定のコピー
FEREC 状態表示
FEREC 管理
Center2 設定
Center2 状態表示
Center2 管理

FEREC 設定 > アクセスコントロール

アクセスコントロール

FTPプロキシ一括設定 グループ単位で FTP プロキシの設定を行います。

5.2.1. FTP プロキシ一括設定

FTP プロキシ一括設定では、グループ登録した FEREC に一括して FTP プロキシを設定することができます。

FEREC において、通常は FTP プロキシを「使用する」の状態で使用してください。

FTP プロキシを使用する場合、LAN 側のクライアント PC、スタティック NAT やスタティックブリッジされた端末はブリッジ/NAT/NAPT のいずれでも、FTP のアクティブモードもパッシブモードもどちらでも使用できます。

但し FTP プロキシを使用する場合、ブリッジ/NAT モードでの全端末と NAPT モードでのスタティック NAT された端末からの制御コネクションはクライアントの(WAN 側)アドレスからではなく FEREC 本体の(WAN 側)アドレスから張られるように、つまり制御コネクションだけが NAPT されているように見えます。

プロキシする制御コネクションのポートは TCP21 番です。

FTP プロキシを使用しない場合、FEREC は制御コネクションについて一切関知しませんので、アクセスコントロールの設定によって適切にデータコネクションが通過できるように設定する必要があります。

- 手順 1： ［FTP プロキシ一括設定］画面を開く

　Center2 管理ページより、［FEREC 設定］→［アクセスコントロール］→［FTP プロキシ一括設定］画面を開きます。

FEREC Center2
バージョン: Center2-2.1

▸ Top
▾ FEREC 設定
ネットワーク
アクセスコントロール
FTPプロキシ一括設定
認証
クライアント設定
認証ページ設定
システム設定
設定のコピー
▸ FEREC 状態表示
▸ FEREC 管理
▸ Center2 設定
▸ Center2 状態表示

FEREC 設定 > アクセスコントロール > FTPプロキシ一括設定

FTPプロキシ一括設定

グループ	0（東棟）
FTP プロキシ設定	使用する

設定　設定が変更された FEREC は自動的に再起動します

- 通常は FTP プロキシを「使用する」の状態で使用してください。
- FTP プロキシを使用する場合、LAN 側のクライアント PC、スタティック NAT やスタティックブリッジされた端末は ブリッジ/NAT/NAPT のいずれでも、FTP のアクティブモードもパッシブモードもどちらでも使用できます。
- ただし FTP プロキシを使用する場合、ブリッジ/NAT モードでの全端末と NAPT モードでのスタティック NAT された端末からの制御コネクションはクライアントの（WAN側）アドレスからではなく FEREC 本体の（WAN側）アドレスから張られるように、つまり制御コネクションだけが NAPT されているように見えます。
- プロキシする制御コネクションのポートは TCP 21 番です。
- FTP プロキシを使用しない場合、FEREC は制御コネクションについて一切関知しませんので、アクセスコントロールの設定によって適切にデータコネクションが通過できるように設定する必要があります。

グループ 0（東棟）に所属している FEREC の FTP プロキシの設定を表示します。

ノード ID	FTP プロキシ
0	使用する

- 手順 2: グループの選択

　［グループ］のプルダウンメニューから、FTP プロキシを設定するグループを選択します。

- 手順 3: 使用有無の設定

　［FTP プロキシ設定］のプルダウンメニューから「使用する」、「使用しない」を選択します。

- 手順 4: 設定

　［設定］ボタンを押すとグループに属する全 FEREC に指定した内容で設定します。設定が変更された FEREC は、自動的に再起動します。

5.3. 認証

認証には、以下の機能があります。

機能	概要
優先順位一括設定	グループ単位で認証に使用するサーバを選択し、その順位の設定を行います。
RADIUS 認証一括設定	グループ単位で RADIUS 認証の設定を行います。
LDAP 認証一括設定	グループ単位で LDAP 認証の設定を行います。
内部認証一括設定	グループ単位で内部認証の設定を行います。
禁止アカウント一括設定	グループ単位でログインを禁止するアカウントの設定を行います。

5.3.1. 優先順位一括設定

優先順位一括設定では、グループ登録した FEREC に一括して使用する認証方式の優先順位を設定します。

- **手順 1：［優先順位一括設定］画面を開く**

  Center2 管理ページより、［FEREC 設定］→［認証］→［優先順位一括設定］画面を開きます。

FEREC Center2　バージョン: Center2-2.1

▸ Top
▾ FEREC 設定
ネットワーク
アクセスコントロール
認証
優先順位一括設定
RADIUS認証一括設定
LDAP認証一括設定
内部認証一括設定
禁止アカウント一括設定
クライアント設定
認証ページ設定
システム設定
設定のコピー
▸ FEREC 状態表示
▸ FEREC 管理

FEREC 設定 > 認証 > 優先順位一括設定

優先順位一括設定

グループ	0（東棟）
優先順位1	(なし)
優先順位2	(なし)
優先順位3	(なし)
優先順位4	(なし)
優先順位5	(なし)

設定

グループ 0（東棟）に所属している FEREC の優先順位の設定を表示します。

ノード ID	優先順位1	優先順位2	優先順位3	優先順位4	優先順位5
0	内部				
1	内部				

- **手順 2: グループの選択**

  ［グループ］のプルダウンメニューから、優先順位を設定するグループを選択します。

- **手順 3: 認証方式の選択**

  ［優先順位 1］のプルダウンメニューから設定する認証方式を選択し指定します。使用する認証方式の数に応じて、以後順に［優先順位 2］から［優先順位 5］まで設定します。使用する認証方式が 5 個に満たない場合、残りは「(なし)」を選択します。

- **手順 4: 設定**

  ［設定］ボタンを押すと、グループに属する全 FEREC に使用する認証方式を指定した順に設定します。

5.3.2. RADIUS 認証一括設定

RADIUS 認証一括設定では、グループ登録した FEREC に一括して RADIUS 認証に使用する RADIUS サーバを設定します。

RADIUS サーバを設定する場合

● 手順 1：［RADIUS 認証一括設定］画面を開く

Center2 管理ページより、［FEREC 設定］→［認証］→［RADIUS 認証一括設定］画面を開きます。

● 手順 2: グループの選択

［グループ］のプルダウンメニューから、RADIUS サーバを設定するグループを選択します。

● 手順 3: 設定対象の選択

［設定対象］のプルダウンメニューから、設定対象を選択します。

● 手順 4: サーバ名の設定

［サーバ名］欄に RADIUS サーバのホスト名または IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

- 手順 5: ポート番号の設定

 ［ポート番号］欄に RADIUS サーバのポート番号を設定します。ポート番号は半角数字で記入します。前後に空白文字が入らないようにしてください。通常使用されるポート番号は 1812 か 1645 です。

- 手順 6: シークレットの設定

 ［シークレット］欄に RADIUS サーバのシークレットを設定します。シークレットは半角 1 文字以上 127 文字以下で記入します。

- 手順 7: タイムアウトの設定

 ［タイムアウト］欄に RADIUS サーバへの接続と認証のタイムアウト値を設定します。タイムアウトは 1～60 秒の範囲から半角数字で記入します。前後に空白文字が入らないようにしてください。

- 手順 8: 既定ポリシーの選択

 RADIUS サーバ側でアクセスポリシーの指定がない場合に利用するアクセスポリシーを［既定ポリシー］プルダウンメニューから選択します。

NOTE

- RADIUS サーバで、“Filter-ID” の属性でポリシー名を指定することによりユーザ毎のアクセスポリシーの振り分けが可能になります。

- 手順 9: MAC アドレス制限の選択

 ［MAC アドレス制限］のプルダウンメニューから「使用する」か「使用しない」かを選択します。通常の RADIUS ユーザ認証に加え、クライアントの MAC アドレス認証も行う場合は、「使用する」を選択します。

- 手順 10: MAC アドレス制限用パスワードの設定

 ［MAC アドレス制限用パスワード］欄に MAC アドレス制限用のパスワードを設定します。パスワードは半角 1 文字以上 127 文字以下で記入します。

- 手順 11: 設定

 ［設定］ボタンを押すと、グループに属する全 FEREC に RADIUS サーバの設定が行われます。

RADIUS サーバの設定を削除する場合

- 手順 1：［RADIUS 認証一括設定］画面を開く
  Center2 管理ページより、［FEREC 設定］→［認証］→［RADIUS 認証一括設定］画面を開きます。

- 手順 2: グループの選択
  ［グループ］のプルダウンメニューから、RADIUS サーバの設定を削除するグループを選択します。

- 手順 3: 設定対象の選択
  ［設定対象］のプルダウンメニューから、設定を削除する対象を選択します。

- 手順 4: サーバ名のクリア
  ［サーバ名］欄を空にします。

- 手順 5: 設定
  ［設定］ボタンを押すと、グループに属する全 FEREC で RADIUS サーバの設定が削除されます。

5.3.3. LDAP 認証一括設定

LDAP 認証一括設定では、グループ登録した FEREC に一括して LDAP 認証に使用する LDAP サーバを設定します。

バインド方式は、「間接バインド」か「直接バインド」が使用できます。間接バインドは、バインド DN でバインドし、ユーザを検索してから再びバインドする方式です。一方、直接バインドは直接ユーザの DN でバインドする方式です。

通常は「間接バインド」を使用します。

LDAP サーバを間接バインド方式で設定する場合

- 手順 1：［LDAP 認証一括設定］画面を開く

  Center2 管理ページより、［FEREC 設定］→［認証］→［LDAP 認証一括設定］画面を開きます。

- 手順 2: バインド方式の選択

  ［バインド方式］プルダウンメニューから、「間接バインド」を選択します。

- 手順 3: グループの選択

  ［グループ］のプルダウンメニューから、LDAP サーバを設定するグループを選択します。

- **手順 4: 設定対象の選択**

  ［設定対象］のプルダウンメニューから、設定対象を選択します。

- **手順 5: サーバ名の設定**

  ［サーバ名］欄に LDAP サーバのホスト名または IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

- **手順 6: ポート番号の設定**

  ［ポート番号］欄に LDAP サーバのポート番号を設定します。ポート番号は半角数字で記入します。前後に空白文字が入らないようにしてください。ポート番号を省略した場合は、プロトコルが LDAP なら 389 番、プロトコルが LDAPS なら 636 番となります。

- **手順 7: プロトコルの選択**

  ［プロトコル］のプルダウンメニューから、LDAP を利用するか LDAPS を利用するかを選択します。

NOTE

- FEREC では、LDAPS（LDAP over SSL）には対応していますが、LDAP over TLS には対応しておりません。

- **手順 8: バインド DN の設定**

  ［バインド DN］欄にユーザ DN を検索するためのバインドに使用するバインド DN を設定します。バインド DN は半角 255 文字以内で記入します。

- **手順 9: バインドパスワードの設定**

  ［バインドパスワード］欄にユーザ DN を検索するためのバインドに使用するバインドパスワードを設定します。バインドパスワードは半角 63 文字以内で記入します。

- **手順 10: ベース DN の設定**

  ［ベース DN］欄にユーザ DN を検索する時のベース DN を設定します。ベース DN 以下のツリーすべてが検索の対象になります。ベース DN は、半角 255 文字以内で記入します。

● 手順 11: タイムアウトの設定

［タイムアウト］欄に LDAP サーバへの接続と認証のタイムアウトを設定します。タイムアウトは 1～60 秒の範囲から半角数字で記入します。前後に空白文字が入らないようにしてください。

● 手順 12: アカウント名属性の設定

［アカウント名属性］欄にユーザを検索する際の属性名を設定します。属性名は半角 1 文字以上 31 文字以下で記入します。例えば、dc=example, dc=jp という DN 以下から cn=Taro というユーザを検索する場合、アカウント名属性には cn を記入します。

● 手順 13: ポリシー名属性の設定

［ポリシー名属性］欄に、FEREC のアクセスポリシー名として使用する属性の属性名を設定します。属性は、バインドするユーザのエントリから選択します。属性名は半角 31 文字以内で記入します。

省略した場合はユーザごとのポリシー指定は行われず、このサーバの既定ポリシー(次項)が適用されます。

また指定の属性名がエントリに存在しない、あるいは取得した値と同名のポリシー名が FEREC に存在しない場合も既定ポリシーが適用されます。

● 手順 14: 既定ポリシーの選択

LDAP サーバ側でアクセスポリシーの指定がない場合に適用するアクセスポリシーを［既定ポリシー］プルダウンメニューから選択します。

● 手順 15: バージョンの選択

LDAP プロトコルのバージョンを、［バージョン］プルダウンメニューから選択します。バージョンは、「2」（LDAPv2）か、または、「3」（LDAPv3）を選択します。初期状態は LDAPv2 です。

● 手順 16: 設定

［設定］ボタンを押すと、グループに属する全 FEREC に LDAP サーバの設定が行われます。

LDAP サーバを直接バインド方式で設定する場合

● 手順 1：［LDAP 認証一括設定］画面を開く

Center2 管理ページより、［FEREC 設定］→［認証］→［LDAP 認証一括設定］画面を開きます。

- 手順 2: バインド方式の選択

  ［バインド方式］プルダウンメニューから、「直接バインド」を選択します。

- 手順 3: グループの選択

  ［グループ］のプルダウンメニューから、LDAP サーバを設定するグループを選択します。

- 手順 4: 設定対象の選択

  ［設定対象］のプルダウンメニューから、設定対象を選択します。

- 手順 5: サーバ名の設定

  ［サーバ名］欄に LDAP サーバのホスト名または IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

- 手順 6: ポート番号の設定

  ［ポート番号］欄に LDAP サーバのポート番号を設定します。ポート番号は半角数字で記入します。前後に空白文字が入らないようにしてください。ポート番号を省略した場合は、プロトコルが LDAP なら 389 番、プロトコルが LDAPS なら 636 番となります。

- 手順 7: プロトコルの選択

  ［プロトコル］のプルダウンメニューから、LDAP を利用するか LDAPS を利用するかを選択します。

NOTE

- FEREC では、LDAPS（LDAP over SSL）には対応していますが、LDAP over TLS には対応しておりません。

- 手順 8: ベース DN の設定

  ［ベース DN］欄にユーザ DN を直接バインドするベース DN を設定します。ベース DN は半角 255 文字以内で記入します。

- 手順 9: タイムアウトの設定

  ［タイムアウト］欄に LDAP サーバへの接続と認証のタイムアウトを設定します。タイムアウトは 1～60 秒の範囲から半角数字で記入します。前後に空白文字が入らないようにしてください。

● 手順 10: アカウント名属性の設定

［アカウント名属性］欄にユーザをバインドする際の属性名を設定します。属性名は半角 1 文字以上 31 文字以下で記入します。例えば、cn=Taro, dc=example, dc=jp という DN でバインドする場合、アカウント名属性には cn を記入します。

● 手順 11: ポリシー名属性の設定

［ポリシー名属性］欄に、FEREC のアクセスポリシー名として使用する属性の属性名を設定します。属性は、バインドするユーザのエントリから選択します。属性名は半角 31 文字以内で記入します。

省略した場合はユーザごとのポリシー指定は行われず、このサーバの既定ポリシー(次項)が適用されます。

また指定の属性名がエントリに存在しない、あるいは取得した値と同名のポリシー名が FEREC に存在しない場合も既定ポリシーが適用されます。

● 手順 12: 既定ポリシーの選択

LDAP サーバ側でアクセスポリシーの指定がない場合に適用するアクセスポリシーを［既定ポリシー］プルダウンメニューから選択します。

● 手順 13: バージョンの選択

LDAP プロトコルのバージョンを、[バージョン]プルダウンメニューから選択します。バージョンは、「2」(LDAPv2) か、または、「3」(LDAPv3) を選択します。初期状態は LDAPv2 です。

● 手順 14: 設定

［設定］ボタンを押すと、グループに属する全 FEREC に LDAP サーバの設定が行われます。

LDAP サーバの設定を削除する場合

● 手順 1：［LDAP 認証一括設定］画面を開く

Center2 管理ページより、［FEREC 設定］→［認証］→［LDAP 認証一括設定］画面を開きます。

● 手順 2: グループの選択

［グループ］のプルダウンメニューから、LDAP サーバの設定を削除するグループを選択します。

- **手順 3: 設定対象の選択**

  ［設定対象］のプルダウンメニューから、設定を削除する対象を選択します。

- **手順 4: サーバ名のクリア**

  ［サーバ名］欄を空にします。

- **手順 5: 設定**

  ［設定］ボタンを押すと、グループに属する全 FEREC で LDAP サーバの設定が削除されます。

5.3.4. 内部認証一括設定

内部認証一括設定では、グループ登録した FEREC に一括して内部認証で使用するアカウントを設定します。内部認証は FEREC 内部に認証用のデータを保持しておくもので、認証サーバのない小規模な環境や、一時的なアカウントの発行に利用できます。

新しいアカウントを追加する場合

● 手順 1：［内部認証一括設定］画面を開く

Center2 管理ページより、［FEREC 設定］→［認証］→［内部認証一括設定］画面を開きます。

● 手順 2: グループの選択

［グループ］のプルダウンメニューから、アカウントを設定するグループを選択します。

● 手順 3: アカウント名の設定

［アカウント名］欄にユーザのアカウント名を設定します。アカウント名は半角 1 文字以上 31 文字以下で記入します。

- **手順 4: パスワードの設定**

［パスワード］欄にユーザのパスワードを設定します。パスワードは半角 3 文字以上 31 文字以下で記入します。

- **手順 5: コメントの設定**

［コメント］欄にアカウントに関するコメントを設定します。コメントは半角 31 文字（全角 15 文字相当）以内で記入します。また、コメントは省略できます。

- **手順 6: ポリシーの選択**

ユーザの認証通過後に適用するポリシーを設定します。ポリシーは、［ポリシー］プルダウンメニューから番号で選択します。

- **手順 7: 追加**

［追加］ボタンを押すと、グループに属する全 FEREC に新しいアカウントとして追加されます。

アカウントを削除する場合

- **手順 1：［内部認証一括設定］画面を開く**

Center2 管理ページより、［FEREC 設定］→［認証］→［内部認証一括設定］画面を開きます。

- **手順 2: グループの選択**

［グループ］のプルダウンメニューから、アカウントを削除するグループを選択します。

- **手順 3: アカウント名の設定**

［アカウント名］欄に削除するユーザのアカウント名を設定します。

- **手順 4: 削除**

［削除］ボタンを押すと、グループに属する全 FEREC でアカウントが削除されます。

5.3.5. 禁止アカウント一括設定

禁止アカウント一括設定では、グループ登録した FEREC に一括してクライアント PC からの利用を禁止するアカウントを設定します。これにより、認証サーバの設定を変更することなく、特定のアカウントの利用を一時的に禁止することができます。

禁止アカウントを追加する場合

- **手順 1：［禁止アカウント一括設定］画面を開く**

  Center2 管理ページより、［FEREC 設定］→［認証］→［禁止アカウント一括設定］画面を開きます。

- **手順 2: グループの選択**

  ［グループ］のプルダウンメニューから、禁止アカウントを設定するグループを選択します。

- **手順 3: アカウント名の設定**

  ［アカウント名］欄に禁止するユーザアカウント名を設定します。アカウント名は半角 1 文字以上 31 文字以下で記入します。

- **手順 4: 追加**

［追加］ボタンを押すと、グループに属する全 FEREC に禁止アカウントとして追加されます。

禁止アカウントを削除する場合

- **手順 1：［禁止アカウント一括設定］画面を開く**

Center2 管理ページより、［FEREC 設定］→［認証］→［禁止アカウント一括設定］画面を開きます。

- **手順 2: グループの選択**

［グループ］のプルダウンメニューから、禁止アカウントを削除するグループを選択します。

- **手順 3: アカウント名の設定**

［アカウント名］欄に削除するユーザのアカウント名を設定します。

- **手順 4: 削除**

［削除］ボタンを押すと、グループに属する全 FEREC で禁止アカウントから削除されます。

5.4. クライアント設定

クライアント設定には、以下の機能があります。

機能	概要
HTTP 外部プロキシ一括設定	グループ単位でプロキシ使用時に認証ページを強制表示するための設定を行います。
重複ログイン一括設定	グループ単位で同一ユーザによる複数 IP アドレスからのログインを許可するかどうかの設定を行います。
ポーリング間隔一括設定	グループ単位でクライアントをポーリングする間隔の設定を行います。
利用時間帯制限一括設定	グループ単位でユーザの利用時間帯制限の設定を行います。

5.4.1. HTTP 外部プロキシ一括設定

HTTP 外部プロキシ一括設定では、グループ登録した FEREC に一括して HTTP 外部プロキシの使用有無を設定できます。

HTTP 外部プロキシ設定を使用すると、クライアント PC において HTTP プロキシを使用した場合でも HTTP プロキシを使用しない場合と同様に、FEREC 認証ページを強制的に表示することができます。

NOTE

- 本機能は、クライアント PC の HTTP プロキシ設定を代替するものではありません。

- 手順 1： ［HTTP 外部プロキシ一括設定］画面を開く

  Center2 管理ページより、［FEREC 設定］→［クライアント設定］→［HTTP 外部プロキシ一括設定］画面を開きます。

- 手順 2: グループの選択

  ［グループ］のプルダウンメニューから、HTTP 外部プロキシを設定するグループを選択します。

- 手順 3: 外部プロキシ設定の選択

［外部プロキシ設定］プルダウンメニューから、「使用する」または「使用しない」を選択します。

- 手順 4: 設定

［設定］ボタンを押すとグループに属する全 FEREC に指定した内容で設定します。設定が変更された FEREC は、自動的に再起動します。

5.4.1.1. プロキシサーバ一括設定

プロキシサーバ一括設定では、グループ登録した FEREC に一括して HTTP 外部プロキシで使用する HTTP プロキシサーバを設定します。

- 手順 1：［プロキシサーバ一括設定］画面を開く

  Center2 管理ページより、［FEREC 設定］→［クライアント設定］→［HTTP 外部プロキシ一括設定］→［プロキシサーバ一括設定］画面を開きます。

- 手順 2: グループの選択

  ［グループ］のプルダウンメニューから、プロキシサーバを設定するグループを選択します。

- 手順 3: プロキシサーバの設定

  使用する HTTP プロキシサーバの数に応じて、プロキシサーバ 1 からプロキシサーバ 5 までの IP アドレスとポート番号を設定します。IP アドレスは半角で記入します。ポート番号は、1～65535 の範囲から半角数字で記入します。IP アドレス、ポート番号はいずれも前後に空白文字が入らないようにしてください。

- 手順 4: 設定

［設定］ボタンを押すとグループに属する全 FEREC に指定した内容で設定します。FEREC は、状態によって自動的に再起動します。

NOTE

- “5.4.1. HTTP外部プロキシ一括設定”の外部プロキシ設定を「使用しない」に設定している場合、FERECは再起動を行いません。(但し、所属しているFERECのバージョンが 2.3 以降の場合に限ります)
- プロキシサーバの設定が変更されていない場合、FEREC は再起動を行いません。

5.4.2. 重複ログイン一括設定

重複ログイン一括設定では、グループ登録した FEREC に一括して重複ログインを許可できます。

通常、FEREC では複数の IP アドレスから同一のアカウントで重複してログインすることはできませんが、これを許可することができます。

工場出荷時、重複ログインは禁止しています。

- 手順 1：［重複ログイン一括設定］画面を開く

  Center2 管理ページより、［FEREC 設定］→［クライアント設定］→［重複ログイン一括設定］画面を開きます。

- 手順 2: グループの選択

  ［グループ］のプルダウンメニューから、重複ログインを設定するグループを選択します。

- 手順 3: 重複ログイン設定の選択

  ［重複ログイン］プルダウンメニューから、「禁止する」または「許可する」を選択します。

- 手順 4: 設定

  ［設定］ボタンを押すとグループに属する全 FEREC に指定した内容で設定します。

5.4.3. ポーリング間隔一括設定

ポーリング間隔一括設定では、グループ登録した FEREC に一括してポーリング間隔を設定できます。

FEREC では、ポーリング間隔で設定された間隔でクライアント PC の生存を確認しています。生存が確認できなかったクライアント PC は、ログアウトしたと見なします。なお、生存確認は、ARP 要求をクライアント PC に送信し、応答があるかどうかで行っています。

工場出荷時、ポーリング間隔は 120 秒に設定されています。

- **手順 1：［ポーリング間隔一括設定］画面を開く**

  Center2 管理ページより、［FEREC 設定］→［クライアント設定］→［ポーリング間隔一括設定］画面を開きます。

- **手順 2: グループの選択**

  ［グループ］のプルダウンメニューから、ポーリング間隔を設定するグループを選択します。

- **手順 3: ポーリング間隔の設定**

  ［ポーリング間隔］欄にポーリング間隔を設定します。ポーリング間隔は 10～600 秒の範囲内で 1 秒単位に半角数字で記入します。前後に空白文字が入らないようにしてください。

- **手順 4: 設定**

［設定］ボタンを押すと、グループに属する全 FEREC でポーリング間隔の設定が指定した秒数に変更されます。

5.4.4. 利用時間帯制限一括設定

利用時間帯制限一括設定では､グループ登録した FEREC に一括してクライアント PC からの利用時間帯を制限させることができます。

すべてのクライアント PC 共通で、利用可能な時間帯を 1 組、5 分単位で指定することができます。利用開始時刻の方が利用終了時刻より遅い場合は、利用可能な時間は翌日にかけた指定になります。なお、利用可能時間内に FEREC で認証を受けていても、利用可能時間を過ぎたら利用できなくなります。

工場出荷時、利用時間帯制限はありません。

利用時間帯を制限する場合

- 手順 1：［利用時間帯制限一括設定］画面を開く

Center2 管理ページより、［FEREC 設定］→［クライアント設定］→［利用時間帯制限一括設定］画面を開きます。

- 手順 2: グループの選択

［グループ］のプルダウンメニューから、利用時間帯を制限するグループを選択します。

- **手順 3: 利用時間帯制限の選択**

  ［利用時間帯制限］のプルダウンメニューから「使用する」を選択します。

- **手順 4: 利用開始時刻の選択**

  ［利用開始時刻］のプルダウンメニューから開始時刻を選択します。

- **手順 5: 利用終了時刻の選択**

  ［利用終了時刻］のプルダウンメニューから終了時刻を選択します。

- **手順 6: 設定**

  ［設定］ボタンを押すと、グループに属する全 FEREC で利用時間帯が制限されます。

利用時間帯制限を解除する場合

- **手順 1：［利用時間帯制限一括設定］画面を開く**

  Center2 管理ページより、［FEREC 設定］→［クライアント設定］→［利用時間帯制限一括設定］画面を開きます。

- **手順 2: グループの選択**

  ［グループ］のプルダウンメニューから、利用時間帯の制限を解除するグループを選択します。

- **手順 3: 利用時間帯制限の選択**

  ［利用時間帯制限］のプルダウンメニューから「使用しない」を選択します。

- **手順 4: 設定**

  ［設定］ボタンを押すと、グループに属する全 FEREC で利用時間帯の制限が解除されます。

5.5. 認証ページ設定

認証ページ設定には、以下の機能があります。

機能	概要
ロゴ表示一括設定	グループ単位で FEREC ロゴの表示、非表示を設定します。
メッセージカタログ一括設定	グループ単位で認証ページに表示されるメッセージを設定します。
アクション一括設定	グループ単位で認証後のページの動作を指定します。

FEREC Center2
バージョン: Center2-2.1

▸ Top
▾ FEREC 設定
ネットワーク
アクセスコントロール
認証
クライアント設定
認証ページ設定
ロゴ表示一括設定
メッセージカタログ一括設定
アクション一括設定
システム設定
設定のコピー
▸ FEREC 状態表示
▸ FEREC 管理
▸ Center2 設定

FEREC 設定 > 認証ページ設定

認証ページ設定

ロゴ表示一括設定 グループ単位で FEREC ロゴの表示、非表示を設定します。

メッセージカタログ一括設定 グループ単位で認証ページに表示されるメッセージを設定します。

アクション一括設定 グループ単位で認証後のページの動作を指定します。

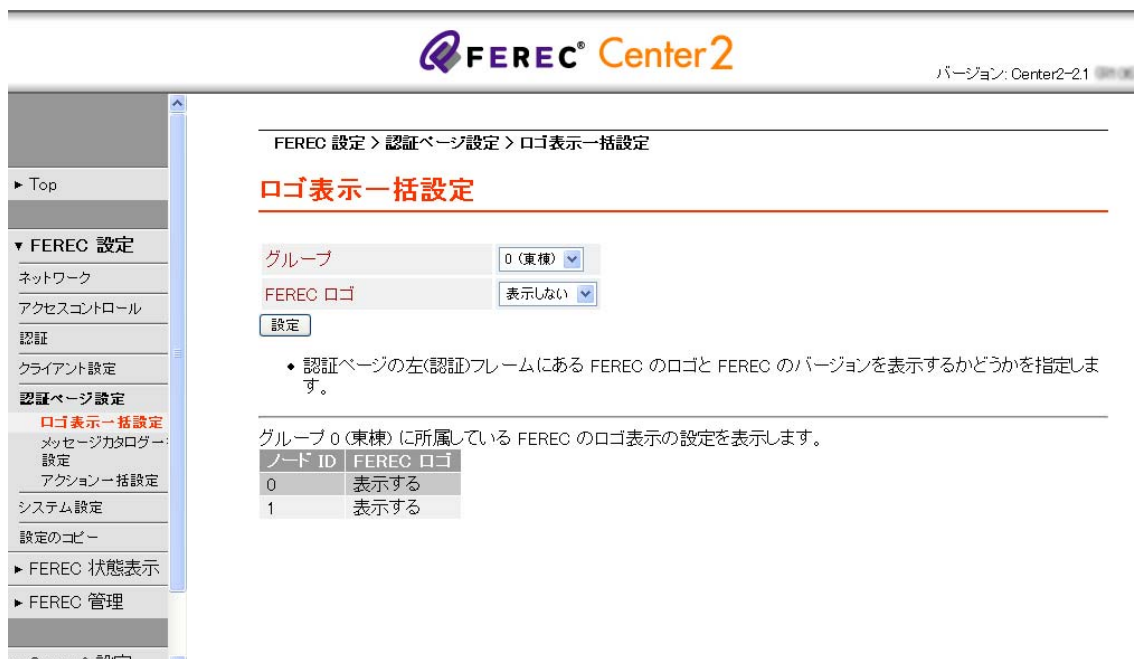
5.5.1. ロゴ表示一括設定

ロゴ表示一括設定では、グループ登録した FEREC に一括してクライアント PC の認証ページに表示される左フレームにある FEREC のロゴと FEREC のバージョンを非表示にできます。FEREC のバージョンや FEREC であることそれ自体をユーザに意識させたくない時には、非表示に変更してお使いください。

工場出荷時は、表示する設定になっています。

ロゴ非表示に変更する場合

- 手順 1：［ロゴ表示一括設定］画面を開く

  Center2 管理ページより、［FEREC 設定］→［認証ページ設定］→［ロゴ表示一括設定］画面を開きます。

- 手順 2: グループの選択

  ［グループ］のプルダウンメニューから、ロゴ表示を変更するグループを選択します。

- 手順 3: ロゴ表示の選択

  ［FEREC ロゴ］のプルダウンメニューから「表示しない」を選択します。

- 手順 4: 設定

　［設定］ボタンを押すと、グループに属する全 FEREC でロゴが非表示に変更されます。

ロゴ表示に戻す場合

- 手順 1：［ロゴ表示一括設定］画面を開く

　Center2 管理ページより、［FEREC 設定］→［認証ページ設定］→［ロゴ表示一括設定］画面を開きます。

- 手順 2: グループの選択

　［グループ］のプルダウンメニューから、ロゴ表示を戻すグループを選択します。

- 手順 3: ロゴ表示の選択

　［FEREC ロゴ］のプルダウンメニューから「表示する」を選択します。

- 手順 4: 設定

　［設定］ボタンを押すと、グループに属する全 FEREC でロゴ表示ありに戻されます。

5.5.2. メッセージカタログ一括設定

メッセージカタログ一括設定では、グループ登録した FEREC に一括してクライアント PC の認証画面に表示するいくつかのメッセージを変更することができます。

変更可能なメッセージは、以下になります。

変更可能メッセージ一覧

識別子	既定メッセージ	説明
username	ユーザ名	認証画面のユーザ名入力フォームの名称を指定します。
password	パスワード	認証画面のパスワード入力フォームの名称を指定します。
login-button	ログイン	認証画面のログインボタンの名称を指定します。
logout-button	ログアウトする	ログアウト画面のログアウトボタンの名称を指定します。
auth-success	認証に成功しました。	認証に成功した時のメッセージを指定します。
client-unknown-ip	クライアント用 IP アドレスが不明です。	クライアントの IP アドレスが取得できなかった場合です。
client-out-of-service	利用時間外です。	利用時間帯制限によって利用を禁止されている時間帯です。
client-out-of-range	クライアント用アドレスの範囲外です。	クライアントの IP アドレスが FEREC の対象とするアドレス範囲外です。
already-login	ログイン中です。	ログインしているユーザが再度認証ページを表示した時のメッセージです。
logout-success	ログアウトに成功しました。3 秒後に認証ページに戻ります。	ログアウトに成功した時です。

（続く）

変更可能メッセージ一覧（続き）

識別子	既定メッセージ	説明
logout-failed	ログアウトに失敗しました。	ログアウトに失敗した時です。
auth-progress	認証しています...	認証サーバに問い合わせ中に表示するメッセージです。
auth-failed-already	{user} さんはすでにログインしています。(*1)	すでにログインしている同じ端末から同じユーザがログインを試みた場合です。エラーではありません。
auth-failed-multi	{user} さんはすでにログインしています。(*1)	重複ログインが禁止されていて、すでに他の端末などからログインしているユーザがログインを試みた場合です。
auth-failed-portlimit	{user} さんは同時ログインの最大数を超えました。(*1)	重複ログインが許可されていますが、その同時ログイン数を超えた場合です。
auth-failed-cred	認証に失敗しました。 ユーザ名かパスワードが違います。	ユーザ名かパスワードが違う場合です。
auth-failed-empty	ユーザ名が入力されていません。 ユーザ名を入力してください。	ユーザ名が入力されていない場合です。
auth-failed-timeout	認証に失敗しました。 認証サーバへの接続がタイムアウトしました。 管理者に連絡してください。	認証サーバへの接続がタイムアウトした場合です。
auth-failed-unreach	認証に失敗しました。 認証サーバに接続できません。 管理者に連絡してください。	RADIUS、LDAP 認証サーバに接続できなかった場合です。
auth-failed-protocol	認証に失敗しました。 認証プロトコルエラーです。 管理者に連絡してください。	認証サーバからの応答が正しく処理できなかった場合です。

（続く）

変更可能メッセージ一覧（続き）

識別子	既定メッセージ	説明
auth-failed-noauth	認証に失敗しました。 認証サーバが指定されていません。 管理者に連絡してください。	認証優先順位で認証サーバが指定されていない場合です。
auth-failed-reject	認証は拒否されました。 ログインは管理者により禁止されています。	禁止アカウントにより認証が禁止されている場合です。
auth-failed-full	ログインできません。 クライアント数の上限に達しています。	クライアント数の上限に達しているためログインできない場合です。
auth-failed-macaddr	認証に失敗しました。 MAC アドレスが登録されていません。	MAC アドレス認証を行っていて、MAC アドレスが登録されていないため認証に失敗した場合です。
auth-failed-internal	認証に失敗しました。 エラーが発生しました。 管理者に連絡してください。	その他のエラーです。

(*1) {user}は、ユーザ名に置き換えて表示されます。

メッセージを変更する場合

- 手順 1：［メッセージカタログ一括設定］画面を開く

  Center2 管理ページより、［FEREC 設定］→［認証ページ設定］→［メッセージカタログ一括設定］画面を開きます。

- 手順 2: グループの選択

  ［グループ］のプルダウンメニューから、メッセージを変更するグループを選択します。

- 手順 3: 識別子の選択

  ［識別子］のプルダウンメニューから、メッセージを変更する識別子を選択します。

- 手順 4: メッセージの選択

  ［メッセージ］のラジオボタンから、「ユーザ定義」を選択します。

- 手順 5: メッセージの入力

  ［ユーザ定義］欄に変更後のメッセージを入力します。メッセージは半角 1 文字以上 200 文字（全角 100 文字相当）以下で記入します。

  auth-failed-already、auth-failed-multi および auth-failed-portlimit のメッセージは、メッセージ中に“{user}”と記述すると、アカウント名に置き換えて表示されます。

● **手順 6: 設定**
［設定］ボタンを押すと、グループに属する全 FEREC で入力した内容にメッセージが変更されます。

メッセージを既定値に戻す場合

● **手順 1：［メッセージカタログ一括設定］画面を開く**
Center2 管理ページより、［FEREC 設定］→［認証ページ設定］→［メッセージカタログ一括設定］画面を開きます。

● **手順 2: グループの選択**
［グループ］のプルダウンメニューから、メッセージを既定値に戻すグループを選択します。

● **手順 3: 識別子の選択**
［識別子］のプルダウンメニューから、メッセージを変更する識別子を選択します。

● **手順 4: メッセージの選択**
［メッセージ］のラジオボタンから、「既定」を選択します。

● **手順 5: 設定**
［設定］ボタンを押すと、グループに属する全 FEREC でメッセージが既定値に戻されます。

5.5.3. アクション一括設定

アクション一括設定では、グループ登録した FEREC に一括してクライアント PC の認証時、認証結果によってカスタムフレームに表示するページを設定できます。

アクション設定で表示するページを変更できるのは以下のケースです。

識別子	説明
success	認証に成功した時。 この時はクライアント情報を左フレーム（認証フレーム）に出力するかどうかについても設定ができます。
fail-passwd	ユーザ名かパスワードが原因で認証に失敗した時
fail-other	それ以外の原因で認証に失敗した時

なお、表示するファイルは HTML エディタ等で作成して頂き、各 FEREC に個別に別途アップロードしてください。アップロード方法については、「FEREC520/720 取扱説明書」をご覧下さい。

認証に成功した時のアクションを変更する場合

- 手順 1：［アクション一括設定］画面を開く

　Center2 管理ページより、［FEREC 設定］→［認証ページ設定］→［アクション一括設定］画面を開きます。

- 手順 2: グループの選択

　［グループ］のプルダウンメニューから、アクションを変更するグループを選択します。

- 手順 3: 識別子の選択

　［識別子］のプルダウンメニューから、アクションを変更する識別子「success」を選択します。

- 手順 4: 動作の選択

　認証に成功した時に右フレームを変更しない場合は、［動作］のラジオボタンで「何もしない」を選択します。

　認証に成功した時に右フレームをアップロードした任意のファイルに切り替える場合は、［動作］のラジオボタンで「右フレームを指定のファイルに変更」を選択し、そのファイル名を入力します。

ファイルはルートディレクトリにあるファイルのみ指定できます。ファイル名は、半角の数字(ASCII コード 0x30～0x39)､英大文字(0x41～0x5a)､英小文字（0x61～0x7a)、ハイフン（0x2d)、ドット（0x2e）およびアンダースコア（0x5f）を使用して、126 文字以内で指定します。

- **手順 5: 左フレームにクライアント情報を出力する機能**

認証に成功した時に、左(認証)フレームにユーザ名などのクライアント情報を出力することができます。機能については「FEREC520/720 取扱説明書」を参照してください。

まず［左フレームにクライアント情報を出力］のプルダウンメニューからこの機能を「使用する」か「使用しない」を選択します。

「使用しない」を選択した場合は個別の項目は指定できません。

「使用する」を選択した場合は、さらに［出力する情報］欄の個別のチェックボックスで出力したい項目を選択します。

- **手順 6: 設定**

［設定］ボタンを押すと、グループに属する全 FEREC のアクション設定が変更されます。

認証に失敗した時のアクションを変更する場合

- **手順 1：［アクション一括設定］画面を開く**

Center2 管理ページより、［FEREC 設定］→［認証ページ設定］→［アクション一括設定］画面を開きます。

- **手順 2: グループの選択**

［グループ］のプルダウンメニューから、アクションを変更するグループを選択します。

- **手順 3: 識別子の選択**

［識別子］のプルダウンメニューから、識別子「fail-passwd」(ユーザ名かパスワードが原因で認証に失敗した時)か「fail-other」(それ以外の原因で認証に失敗した時)を選択します。

- **手順 4: 動作の選択**

認証に失敗した時に右フレームを変更しない場合は、［動作］のラジオボタンで「何もしない」を選択します。

認証に失敗した時に右フレームをアップロードした任意のファイルに切り替えたい場合は、［動作］のラジオボタンで「右フレームを指定のファイルに変更」を選択し、そのファイル名を入力します。ファイル名の制約については前項「認証に成功した時のアクションを変更する場合」を参照してください。

なお、認証に失敗した場合には、クライアント情報の出力は一切行いません。

- **手順 5: 設定**

［設定］ボタンを押すと、グループに属する全 FEREC の設定が変更されます。

5.6. システム設定

システム設定には、以下の機能があります。

機能	概要
管理許可アドレス一括設定	グループ単位で管理許可アドレスの設定を行います。
RADIUS アカウンティング一括設定	グループ単位で RADIUS アカウンティングサーバの設定を行います。
syslog 一括設定	グループ単位でログを転送する syslog サーバの設定を行います。
時刻一括設定	グループ単位で時刻の設定を行います。
管理者パスワード一括設定	グループ単位で管理者パスワードの設定を行います。
FTP パスワード一括設定	グループ単位で FTP パスワードの設定を行います。

5.6.1. 管理許可アドレス一括設定

管理許可アドレス一括設定では、グループ登録した FEREC に一括して管理許可アドレスを設定できます。

FEREC では、管理ページ、管理コンソール（telnet, ssh）およびカスタムページ用の FTP への接続を、許可した特定のアドレスのみに制限することができます。

管理許可アドレスは、最大 5 個まで登録できます。

なお、FEREC の MNT ポートおよび Center2 にはこの管理許可アドレスによる制限は適用されず、常に接続できます。

また、工場出荷時は、制限していません。

管理許可アドレスを追加する場合

- 手順 1：［管理許可アドレス一括設定］画面を開く

  Center2 管理ページより、［FEREC 設定］→［システム設定］→［管理許可アドレス一括設定］画面を開きます。

- 手順 2: グループの選択

  ［グループ］のプルダウンメニューから、管理許可アドレスを追加するグループを選択します。

- 手順 3: 管理許可アドレスの入力

 ［管理許可アドレス］欄に登録する IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。また、ネットマスク長をプルダウンメニューから選択します。管理許可アドレスはネットワークまたは単一ホストで指定します。ネットワーク全体を指定する場合は 192.168.45.0/24 のように CIDR 表記で指定します。単一のホストを指定する場合は 192.168.45.10/32 のようにネットマスク長を 32 にします。

- 手順 4: 追加

 ［追加］ボタンを押すと、グループに属する全 FEREC で管理許可アドレスが追加されます。

管理許可アドレスを削除する場合

- 手順 1：［管理許可アドレス一括設定］画面を開く

 Center2 管理ページより、［FEREC 設定］→［システム設定］→［管理許可アドレス一括設定］画面を開きます。

- 手順 2: グループの選択

 ［グループ］のプルダウンメニューから、管理許可アドレスを削除するグループを選択します。

- 手順 3: 管理許可アドレスの入力

 ［管理許可アドレス］欄に削除するアドレスを半角で記入します。前後に空白文字が入らないようにしてください。また、ネットマスク長をプルダウンメニューから選択します。管理許可アドレスはネットワークまたは単一ホストで指定します。ネットワーク全体を指定する場合は 192.168.45.0/24 のように CIDR 表記で指定します。単一のホストを指定する場合は 192.168.45.10/32 のようにネットマスク長を 32 にします。

- 手順 4: 削除

 ［削除］ボタンを押すと、グループに属する全 FEREC で管理許可アドレスが削除されます。

5.6.2. RADIUS アカウンティング一括設定

RADIUS アカウンティング一括設定では、グループ登録した FEREC に一括して RADIUS アカウンティングサーバを設定できます。RADIUS アカウンティングサーバは、最大 2 台設定できます。なお、両方のサーバを設定した場合には、同じアカウンティング情報を両方のサーバに送信します。

RADIUS アカウンティングサーバを設定する場合

- 手順 1：［RADIUS アカウンティング一括設定］画面を開く

  Center2 管理ページより、［FEREC 設定］→［システム設定］→［RADIUS アカウンティング一括設定］画面を開きます。

- 手順 2: グループの選択

  ［グループ］のプルダウンメニューから、RADIUS アカウンティングサーバを設定するグループを選択します。

- 手順 3: 設定対象の選択

  ［設定対象］のプルダウンメニューから、設定対象を選択します。

- **手順 4: サーバ名の設定**

  RADIUS アカウンティングサーバのホスト名または IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

- **手順 5: ポート番号の設定**

  RADIUS アカウンティングサーバのポート番号を設定します。ポート番号は半角数字で記入します。前後に空白文字が入らないようにしてください。通常使用されるポート番号は 1813 か 1646 です。

- **手順 6: シークレットの設定**

  RADIUS アカウンティングサーバのシークレットを設定します。シークレットは半角 1 文字以上 127 文字以下で記入します。

- **手順 7: タイムアウトの設定**

  RADIUS アカウンティングサーバへの接続とアカウンティング情報送信のタイムアウト値を設定します。タイムアウトは 1～60 秒の範囲から半角数字で記入します。前後に空白文字が入らないようにしてください。

- **手順 8: 設定**

  ［設定］ボタンを押すと、グループに属する全 FEREC で RADIUS アカウンティングサーバの設定が行われます。

RADIUS アカウンティングサーバを削除する場合

- **手順 1：［RADIUS アカウンティング一括設定］画面を開く**

  Center2 管理ページより、［FEREC 設定］→［システム設定］→［RADIUS アカウンティング一括設定］画面を開きます。

- **手順 2: グループの選択**

  ［グループ］のプルダウンメニューから、RADIUS アカウンティングサーバを削除するグループを選択します。

- **手順 3: 設定対象の選択**

  ［設定対象］のプルダウンメニューから、設定を削除する対象を選択します。

- 手順 4: サーバ名のクリア

［サーバ名］欄を空にします。

- 手順 5: 設定

［設定］ボタンを押すと、グループに属する全 FEREC で RADIUS アカウンティングサーバの設定が削除されます。

5.6.3. syslog 一括設定

syslog 一括設定では、グループ登録した FEREC に一括して syslog サーバを設定できます。

FEREC では、自身のログを Center2 とは別に外部の syslog サーバにも送信することができます。

- **手順 1：［syslog 一括設定］画面を開く**

  Center2 管理ページより、［FEREC 設定］→［システム設定］→［syslog 一括設定］画面を開きます。

- **手順 2: グループの選択**

  ［グループ］のプルダウンメニューから、syslog サーバを設定するグループを選択します。

- **手順 3: サーバ名の設定**

  ［サーバ名］欄に syslog サーバのホスト名または IP アドレスを設定します。前後に空白文字が入らないようにしてください。

● 手順 4: ファシリティの選択

［ファシリティ］のプルダウンメニューから syslog サーバへログを送信する際のファシリティを選択します。選択可能なファシリティは、「local0」～「local7」です。

● 手順 5: レベルの選択

［レベル］のプルダウンメニューから syslog サーバへ送信するレベルを選択します。

FEREC は､重大度がここで選択したレベル以上のログを syslog サーバへ送信します。重大度は高い方から順に、「ERR」､「WARN」､「NOTICE」､「INFO」､「DEBUG」となります。

● 手順 6: 設定

［設定］ボタンを押すと、グループに属する全 FEREC で syslog サーバが設定されます。

5.6.4. 時刻一括設定

時刻一括設定では、グループ登録した FEREC に一括して FEREC 本体の時刻を設定します。設定方法は、NTP サーバ指定か直接設定かを選ぶことができます。

NTP サーバを指定する場合

- 手順 1：［時刻一括設定］画面を開く

  Center2 管理ページより、［FEREC 設定］→［システム設定］→［時刻一括設定］画面を開きます。

- 手順 2: グループの選択

  ［グループ］のプルダウンメニューから、時刻を設定するグループを選択します。

- 手順 3: NTP サーバの選択

  ラジオボタンで NTP サーバを選択します。

- 手順 4: サーバの設定

  ［NTP サーバ］欄に NTP サーバもしくは SNTP サーバのホスト名または IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

- **手順 5: 設定**

  ［設定］ボタンを押すと、グループに属する全 FEREC で NTP サーバとの時刻同期を開始します。

時刻を直接設定する場合

- **手順 1：［時刻一括設定］画面を開く**

  Center2 管理ページより、［FEREC 設定］→［システム設定］→［時刻一括設定］画面を開きます。

- **手順 2: グループの選択**

  ［グループ］のプルダウンメニューから、時刻を設定するグループを選択します。

- **手順 3: 直接設定の選択**

  ［直接設定］の左にあるラジオボタンを選択します。

- **手順 4: 時刻の設定**

  ［年］、［月］、［日］、［時］、［分］欄に時刻を設定します。いずれも前後に空白文字が入らないようにしてください。秒は 00 秒になります。

- **手順 5: 設定**

  ［設定］ボタンを押すと、グループに属する全 FEREC で指定した時刻に設定します。

5.6.5. 管理者パスワード一括設定

管理者パスワード一括設定では、グループ登録した FEREC に一括して管理者パスワードを設定します。

管理者パスワードは、管理ページへアクセスおよび管理コンソールへログインする際に使用します。

- 手順 1：［管理者パスワード一括設定］画面を開く

  Center2 管理ページより、［FEREC 設定］→［システム設定］→［管理者パスワード一括設定］画面を開きます。

- 手順 2: グループの選択

  ［グループ］のプルダウンメニューから、管理者パスワードを設定するグループを選択します。

- 手順 3: 管理者パスワードの入力

  ［管理者パスワード］欄に管理者パスワードを入力します。管理者パスワードは半角（ASCII コード 0x20～0x7e）3 文字以上 15 文字以下で記入します。

- 手順 4: 設定

  ［設定］ボタンを押すと、直ちに管理者パスワードが変更されます。

5.6.6. FTP パスワード一括設定

FTP パスワード一括設定では、グループ登録した FEREC に一括して FTP パスワードを設定します。

FTP パスワードは、カスタム領域用の FTP ログインに使用します。

- 手順 1：［FTP パスワード一括設定］画面を開く

  Center2 管理ページより、［FEREC 設定］→［システム設定］→［FTP パスワード一括設定］画面を開きます。

- 手順 2: グループの選択

  ［グループ］のプルダウンメニューから、FTP パスワードを設定するグループを選択します。

- 手順 3: FTP パスワードの入力

  ［FTP パスワード］欄に FTP パスワードを入力します。FTP パスワードは半角（ASCII コード 0x20～0x7e）3 文字以上 15 文字以下で記入します。

- 手順 4: 設定

  ［設定］ボタンを押すと、直ちに FTP パスワードが変更されます。

5.7. 設定のコピー

設定のコピーでは、指定した FEREC からグループ登録した FEREC に設定を一括してコピーします。コピー先の FEREC に既に設定がある場合は削除され、コピー元とコピー先は同一の設定になります。

- **手順 1：［設定のコピー］画面を開く**

  Center2 管理ページより、［FEREC 設定］→［設定のコピー］画面を開きます。

FEREC Center2　バージョン: Center2-2.1

▸ Top
▾ FEREC 設定
ネットワーク
アクセスコントロール
認証
クライアント設定
認証ページ設定
システム設定
設定のコピー
▸ FEREC 状態表示
▸ FEREC 管理
▸ Center2 設定
▸ Center2 状態表示
▸ Center2 管理

FEREC 設定 > 設定のコピー

設定のコピー

指定した FEREC の設定をグループの全 FEREC にコピーします。

コピー元 FEREC	172.16.3.63
コピー先グループ	0（東棟）
コピー対象	すべて

実行

- コピー対象の「すべて」は下記の項目が対象になります。
  - ポリシー
  - 内部認証
  - 禁止アカウント
  - アクション設定
- アクション設定を指定した場合でファイルの指定がある場合は、コンテンツもコピーされます。

- **手順 2: コピー元 FEREC の選択**

  ［コピー元 FEREC］のプルダウンメニューから、コピー元の FEREC を選択します。

- **手順 3: コピー先グループの選択**

  ［コピー先グループ］のプルダウンメニューから、コピー先のグループを選択します。

- **手順 4: コピー対象の選択**

  ［コピー対象］のプルダウンメニューから、コピー対象を選択します。コピー対象は「ポリシー」、「内部認証」、「禁止アカウント」、「アクション設定」および「すべて」から選択します。「すべて」を選択すると、「ポリシー」、「内部認証」、「禁止アカウント」および「アクション設定」をコピーします。

「アクション設定」または「すべて」を選択し、アクション設定で動作が「右フレームを指定のファイルに変更」に設定されている場合は、コンテンツも同時にコピーします。

- **手順 5: 実行**
  ［実行］ボタンを押すと、直ちにコピーが実行されます。

6. FEREC 状態表示

FEREC 状態表示には、以下の機能があります。

機能	概要
FEREC 状態一覧	登録されている FEREC の状態を一覧で表示します。
ログインユーザー一覧	全 FEREC にログインしているユーザの一覧を表示します。
FEREC ログ	FEREC のログを表示します。
FEREC ログイン履歴	FEREC のログイン履歴を表示します。

FEREC Center2
バージョン: Center2-2.1

▸ Top
▸ FEREC 設定
▾ FEREC 状態表示
FEREC状態一覧
ログインユーザー一覧
FERECログ
FERECログイン履歴
▸ FEREC 管理
▸ Center2 設定
▸ Center2 状態表示
▸ Center2 管理

FEREC 状態表示

FEREC 状態表示

FEREC状態一覧 登録されている FEREC の状態を一覧で表示します。

ログインユーザー一覧 全 FEREC にログインしているユーザの一覧を表示します。

FERECログ FEREC のログを表示します。

FERECログイン履歴 FEREC のログイン履歴を表示します。

6.1. FEREC 状態一覧

FEREC 状態一覧では、管理対象 FEREC の各種状態を確認できます。

FEREC の状態を表示する場合

● 手順 1：［FEREC 状態一覧］画面を開く

Center2 管理ページより［FEREC 状態表示］→［FEREC 状態一覧］画面を開くと、管理対象 FEREC の各種状態が表示されます。

FEREC Center2

バージョン: Center2-2.1

FEREC 状態表示 > FEREC状態一覧

FEREC状態一覧

2 台の FEREC が登録されています。

ノード ID	IP アドレス	コメント	状態	型番	ログイン人数	場所	設定の最終更新時刻	シリアル番号	バージョン
Center2 側の情報			FEREC から取得した情報						
0	172.16.3.63	東棟1F	稼働中	FAJ520	1/125	1F	2008-09-25 15:29:35	FAJ-0000-0005	FEREC-2.3
1	172.16.3.65	東棟2F	稼働中	FAJ520	0/125	2F	2008-09-25 14:21:24	FAJ-0000-0006	FEREC-2.3

なお、表示される状態は、以下のとおりです。

Center2 側の情報

項目	内容
ノード ID	管理対象一覧で登録した FEREC のノード ID
IP アドレス	管理対象一覧で登録した FEREC の IP アドレス
コメント	管理対象一覧で登録した FEREC のコメント

FEREC から取得した情報

項目	内容
状態	FEREC の稼働状態
型番	FEREC の型番
ログイン人数	FEREC にログインしているユーザ数／同時にログインできる最大ユーザ数(*)
場所	FEREC の場所名
設定の最終更新時刻	FEREC の設定を最後に更新した時刻
シリアル番号	FEREC のシリアル番号
バージョン	FEREC のバージョン

(*)同時にログインできる最大ユーザ数は FEREC の接続方式によって異なります。
接続方式が NAT または NAPT の場合はアドレス設定のクライアント用アドレスとして予約したアドレス数に、ブリッジモードの場合は同時接続クライアント数（FEREC 520 は 125、FEREC 720 は 250）になります。

ログインユーザを確認する場合

- **手順 1：［FEREC 状態一覧］画面を開く**
  Center2 管理ページより［FEREC 状態表示］→［FEREC 状態一覧］画面を開きます。

- **手順 2: ログインユーザの確認**
  ログイン人数をクリックすると、該当 FEREC にログインしているユーザが確認できます。

FEREC へアクセスする場合

- **手順 1：［FEREC 状態一覧］画面を開く**
  Center2 管理ページより［FEREC 状態表示］→［FEREC 状態一覧］画面を開きます。

- **手順 2: FEREC へのアクセス**
  IP アドレスをクリックすると、該当 FEREC にアクセスできます。
  但し、FEREC の管理許可アドレス設定で、管理ページへのアクセスを制限している場合は、直接 FEREC にアクセスする場合と同様に、管理用 PC を管理許可アドレスに追加する必要があります。

6.2. ログインユーザー覧

ログインユーザー覧では、管理対象 FEREC にログインしているユーザを確認できます。

すべてのログインユーザを表示する場合

- 手順 1：［ログインユーザー覧］画面を開く

  Center2 管理ページより［FEREC 状態表示］→［ログインユーザー覧］画面を開くと、管理対象 FEREC にログインしているユーザが表示されます。

FEREC Center2　バージョン：Center2-2.1

Top / FEREC 設定 / FEREC 状態表示 / FEREC状態一覧 / ログインユーザー覧 / FERECログ / FERECログイン履歴 / FEREC 管理 / Center2 設定 / Center2 状態表示 / Center2 管理

FEREC 状態表示 > ログインユーザー覧

ログインユーザー覧

FEREC すべて

表示

2008-09-25 15:38 現在、合計 1 人がログインしています。

FEREC	IPアドレス	ユーザ名	MACアドレス	ログイン時刻
172.16.3.63	172.16.3.233	guest01	[illegible]	2008-09-25 15:37

表示するログインユーザを選択する場合

- 手順 1：［ログインユーザー覧］画面を開く

  Center2 管理ページより［FEREC 状態表示］→［ログインユーザー覧］画面を開きます。

- 手順 2: 表示対象の選択

  ［FEREC］のプルダウンメニューから、表示対象を選択します。表示対象は「すべて」、「グループ」、および「個別」から選択します。「グループ」、および「個別」の場合は続けてグループまたは FEREC を選択します。

- 手順 3: 表示

  ［表示］ボタンを押すと、該当の FEREC にログインしているユーザが表示されます。

6.3. FEREC ログ

FEREC ログでは、管理対象 FEREC のログを最大 10000 件まで表示できます。また、ログを管理用 PC にダウンロードできます。

NOTE

- ダウンロードされるログは、表示されている内容をそのままダウンロードするのではなく、［ダウンロード］ボタンを押した時点の内容になります。

ログを表示する場合

- 手順 1：［ログ］画面を開く

Center2 管理ページより［FEREC 状態表示］→［FEREC ログ］画面を開くと、ログが表示されます。

ログの表示条件を指定する場合

- 手順 1：［ログ］画面を開く

Center2 管理ページより［FEREC 状態表示］→［FEREC ログ］画面を開きます。

● 手順 2: 表示条件の設定

以下の表示条件を設定することで、ログの表示内容を指定できます。

指定条件	内容
表示開始時刻	表示を開始する時刻を時単位で指定します。初期値は、現在時刻（但し分以下を切り捨て）の 1 時間前です。
表示終了時刻	表示を終了する時刻を時単位で指定します。初期値は、現在時刻（但し分以下を切り捨て）の 1 時間後です。
ログ種別	表示するログの種別を「システムログ」、「ユーザログ」、「パケットログ」、および「デバッグログ」から選択します。初期値は、「システムログ」です。
FEREC	表示する FEREC を選択します。表示対象は、「すべて」、「グループ」、および「個別」から選択します。「グループ」、および「個別」の場合は、続けて、グループまたは FEREC を選択します。初期値は、「すべて」です。

● 手順 3: 表示

［表示］ボタンを押すと、指定した条件でログが表示されます。

ログをダウンロードする場合

● 手順 1：［ログ］画面を開く

Center2 管理ページより［FEREC 状態表示］→［FEREC ログ］画面を開きます。

● 手順 2: ダウンロード条件の設定

ログを表示する場合と同様に条件を設定することで、ダウンロードする内容を指定できます。

● 手順 3: ダウンロード

［ダウンロード］ボタンを押すと、指定した条件でログをダウンロードできます。

6.4. FEREC ログイン履歴

FEREC ログイン履歴では、管理対象 FEREC にログインおよびログアウトしたユーザの履歴を最大 10000 件まで表示できます。また、履歴を管理用 PC にダウンロードできます。

NOTE

- ダウンロードされる履歴は、表示されている内容をそのままダウンロードするのではなく、［ダウンロード］ボタンを押した時点の内容になります。

ログイン履歴を表示する場合

- **手順 1：［ログイン履歴］画面を開く**

  Center2 管理ページより［FEREC 状態表示］→［FEREC ログイン履歴］画面を開くと、ユーザのログイン履歴が表示されます。

FEREC Center2 バージョン: Center2-2.1

▸ Top
▸ FEREC 設定
▾ FEREC 状態表示
FEREC状態一覧
ログインユーザ一覧
FERECログ
FERECログイン履歴
▸ FEREC 管理
▸ Center2 設定
▸ Center2 状態表示
▸ Center2 管理

FEREC 状態表示 > FERECログイン履歴

FERECログイン履歴

表示開始時刻 2008 年 9 月 25 日 14 時
表示終了時刻 2008 年 9 月 25 日 16 時
ユーザ名
FEREC すべて

表示 ダウンロード

日時	FEREC	動作	ユーザ名	クライアント	MACアドレス	ポリシー	認証サーバ	説明
2008-09-25 15:37:56	172.16.3.63	login success	guest01	172.16.3.233	[illegible]	1	guest	

なお、表示される内容は、以下のとおりです。

項目	内容
日時	ログインまたはログアウトを行った日時
FEREC	ログインまたはログアウトを行った FEREC の IP アドレス
動作	“login success”,“login failure”,または“logout”を表示
ユーザ名	ログインまたはログアウトを行ったユーザ名
クライアント	ログインまたはログアウトを行ったクライアントの IP アドレス
MAC アドレス	ログインまたはログアウトを行ったクライアントのMACアドレス
ポリシー	ログイン時に適用したポリシーの番号
認証サーバ	ログイン時にユーザを認証した認証サーバの種別(*)
説明	ログイン失敗時の理由(*)、または、ログアウトの原因(*)

(*)詳しくは、「FEREC520/720 取扱説明書」に記載のユーザログに関する説明をご参照下さい。

ログイン履歴の表示条件を指定する場合

- 手順 1：［ログイン履歴］画面を開く

Center2 管理ページより［FEREC 状態表示］→［FEREC ログイン履歴］画面を開きます。

- 手順 2: 表示条件の設定

以下の表示条件を設定することで、ログイン履歴の表示内容を指定できます。

指定条件	内容
表示開始時刻	表示を開始する時刻を時単位で指定します。初期値は現在時刻（但し分以下を切り捨て）の 1 時間前です。
表示終了時刻	表示を終了する時刻を時単位で指定します。初期値は現在時刻（但し分以下を切り捨て）の 1 時間後です。
ユーザ名	表示するユーザ名を指定します。［指定］ボタンを押すと実際の表示に反映します。空欄の場合はすべてのユーザが表示されます。
FEREC	表示する FEREC を選択します。表示対象は「すべて」、「グループ」、および「個別」から選択します。「グループ」、および「個別」の場合は、続けて、グループまたは FEREC を選択します。初期値は「すべて」です。

- 手順 3: 表示

［表示］ボタンを押すと、指定した条件でログイン履歴が表示されます。

ログイン履歴をダウンロードする場合

- 手順 1：［ログイン履歴］画面を開く

Center2 管理ページより［FEREC 状態表示］→［FEREC ログイン履歴］画面を開きます。

- 手順 2: ダウンロード条件の設定

ログイン履歴を表示する場合と同様に条件を設定することで、ダウンロードする内容を指定できます。

- 手順 3: ダウンロード

［ダウンロード］ボタンを押すと、指定した条件でログイン履歴をダウンロードできます。

7. FEREC 管理

FEREC 管理には、以下の機能があります。

機能	概要
管理対象一覧	登録されている FEREC を管理します。追加、削除、編集もここで行います。
グループ一覧	グループを管理します。追加、削除、編集もここで行います。
一括設定初期化	グループ単位で FEREC の設定を初期化し、工場出荷時状態に戻します。
一括再起動	グループ単位で FEREC の再起動を行います。
一括ステータスダンプ取得	グループ単位で FEREC の障害解析用のステータスダンプを取得します。
一括バックアップ取得	グループ単位で FEREC 設定のバックアップを行います。
一括ファームウェア更新	グループ単位で FEREC のファームウェアの更新を行います。

7.1. 管理対象一覧

管理対象一覧では、Center2 で管理する FEREC の登録、変更、削除および登録済み FEREC の一覧を表示します。

管理対象にできるのは、FEREC520/FEREC720(ファームウェア ver 2.2.2 以降)です。

なお、最大 50 台まで登録可能です。

また、Center2 は、FEREC を管理するためのコネクションを持ちます。コネクションは FEREC から Center2 に対して、TCP、UDP 両方の 6850 番を使用して接続します。

FEREC を管理対象に追加する場合

- 手順 1：［管理対象一覧］画面を開く

  Center2 管理ページより［FEREC 管理］→［管理対象一覧］画面を開きます。

- **手順 2: FEREC の追加画面を開く**

  ［新しい FEREC の追加］ボタンを押して、FEREC の追加画面を開きます。

- **手順 3: ノード ID の選択**

  ［ノード ID］のプルダウンメニューから FEREC を登録するノード ID を選択します。

- **手順 4: IP アドレスの入力**

  ［IP アドレス］欄に登録する FEREC の IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。なお、FEREC の接続方式が NAT または NAPT の場合は、WAN 側インタフェースの IP アドレスを記入します。

- **手順 5: コメントの入力（任意）**

  ［コメント］欄に登録する FEREC に関するコメントを入力します。コメントは半角 31 文字(全角 15 文字相当)以下で記入します。コメントは FEREC の場所名とは別に設定できますので、FEREC の管理者やその連絡先など、FEREC を管理する上で有用な情報を設定してお使い下さい。

- **手順 6: 追加**

  ［追加］ボタンを押すと管理対象とする FEREC が追加されます。

管理対象 FEREC を編集する場合

- **手順 1：［管理対象一覧］画面を開く**
  Center2 管理ページより［FEREC 管理］→［管理対象一覧］画面を開きます。

- **手順 2: FEREC の編集画面を開く**
  FEREC の右にある［編集］ボタンを押して、FEREC の編集画面を開きます。

- **手順 3: IP アドレスの編集**
  ［IP アドレス］欄で FEREC の IP アドレスを編集します。前後に空白文字が入らないようにしてください。

- **手順 4: コメントの編集（任意）**
  ［コメント］欄で登録する FEREC に関するコメントを編集します。

- **手順 5: 設定**
  ［設定］ボタンを押すと管理対象 FEREC の編集結果が反映されます。

FEREC を管理対象から削除する場合

- 手順 1：［管理対象一覧］画面を開く

  Center2 管理ページより［FEREC 管理］→［管理対象一覧］画面を開きます。

- 手順 2: FEREC の削除

  FEREC の右横にある［削除］ボタンを押すと、該当の FEREC が管理対象から削除されます。

NOTE

- 管理対象から削除した FEREC をグループからも削除するには、別途グループの編集で［所属 FEREC］から除外する必要があります。

7.2. グループ一覧

Center2 では、複数の管理対象 FEREC をグループ化し、一括して設定、操作することができます。グループ一覧では、グループの追加、編集、削除および登録済みグループの一覧が表示されます。

なお、最大 32 件まで登録可能です。

NOTE

- グループ内の各 FEREC は、ファームウェアを同じバージョンで揃える必要があります。揃っていない場合、各種一括設定を行った際、エラーになる場合があります。

グループを追加する場合

- 手順 1：［グループ一覧］画面を開く

  Center2 管理ページより［FEREC 管理］→［グループ一覧］画面を開きます。

FEREC Center2　バージョン: Center2-2.1

▸ Top
▸ FEREC 設定
▸ FEREC 状態表示
▾ FEREC 管理
管理対象一覧
グループ一覧
一括設定初期化
一括再起動
一括ステータスダンプ取得
一括バックアップ取得
一括ファームウェア更新
▸ Center2 設定
▸ Center2 状態表示
▸ Center2 管理

FEREC 管理 > グループ一覧

グループ一覧

1 個のグループが登録されています。

新しいグループの追加

グループ ID	コメント	所属台数		
0	東棟	2	編集	削除

- 手順 2: グループの追加画面を開く

［新しいグループの追加］ボタンを押して、グループの追加画面を開きます。

- 手順 3: グループ ID の選択

［グループ ID］のプルダウンメニューからグループを登録するグループ ID を選択します。

- 手順 4: コメントの入力（任意）

［コメント］欄に登録するグループに関するコメントを入力します。コメントは半角 31 文字(全角 15 文字相当)以下で記入します。

- 手順 5: 所属 FEREC の選択

［所属 FEREC］で、このグループに属する FEREC のチェックボックスをチェックして選択します。最上段をチェックするとすべての FEREC を選択できます。

- 手順 6: 追加

［追加］ボタンを押すとグループが追加されます。

グループを編集する場合

● 手順 1：［グループ一覧］画面を開く

Center2 管理ページより［FEREC 管理］→［グループ一覧］画面を開きます。

● 手順 2: グループの編集画面を開く

グループの右にある［編集］ボタンを押して、グループの編集画面を開きます。

● 手順 3: コメントの編集（任意）

［コメント］欄で登録するグループを識別するためのコメントを編集します。

● 手順 4: 所属 FEREC の変更

［所属 FEREC］で、このグループに追加する FEREC のチェックボックスをチェックして選択するか、または、このグループから除く FEREC のチェックを外します。

● 手順 5: 設定

［設定］ボタンを押すとグループの編集結果が反映されます。

グループを削除する場合

- 手順 1：［グループ一覧］画面を開く
  Center2 管理ページより［FEREC 管理］→［グループ一覧］画面を開きます。

- 手順 2: グループの削除
  グループの右横にある［削除］ボタンを押すと、該当のグループが削除されます。

7.3. 一括設定初期化

一括設定初期化では、グループ登録した FEREC を一括して設定を初期化することができます。

- 手順 1: ［一括設定初期化］画面を開く

  Center2 管理ページより［FEREC 管理］→［一括設定初期化］画面を開きます。

- 手順 2: グループの選択

  ［グループ］のプルダウンメニューから、初期化するグループを選択します。

- 手順 3: 初期化

  ［実行］ボタンを押すと、グループに属する全 FEREC の設定を初期化します。実行後、引き続き FEREC を管理するためには、再度、各 FEREC で Center2 を設定する必要があります。

7.4. 一括再起動

一括再起動では、グループ登録した FEREC を一括して再起動することができます。

- **手順 1: ［一括再起動］画面を開く**
  Center2 管理ページより［FEREC 管理］→［一括再起動］画面を開きます。

- **手順 2: グループの選択**
  ［グループ］のプルダウンメニューから、再起動するグループを選択します。

- **手順 3: 再起動**
  ［実行］ボタンを押すと、グループに属する全 FEREC が再起動します。

7.5. 一括ステータスダンプ取得

一括ステータスダンプ取得では、グループ登録した FEREC のステータスダンプを一括して取得することができます。取得できるステータスダンプは、各 FEREC のステータスダンプが zip 形式でひとつのファイルにまとめられています。

- **手順 1: ［一括ステータスダンプ取得］画面を開く**

  Center2 管理ページより［FEREC 管理］→［一括ステータスダンプ取得］画面を開きます。

- **手順 2: グループの選択**

  ［グループ］のプルダウンメニューから、ステータスダンプを取得するグループを選択します。

- **手順 3: ステータスダンプ取得**

  ［実行］ボタンを押すと、グループに属する全 FEREC のステータスダンプを取得します。

7.6. 一括バックアップ取得

一括バックアップ取得では、グループ登録した FEREC のバックアップを一括して取得することができます。取得できるバックアップは、各 FEREC のバックアップ（FEREC のシリアル番号をファイル名とする zip 形式のファイル）が zip 形式でひとつのファイルにまとめられています。

リストアは、リストアする FEREC のバックアップファイルを一括バックアップファイルから前もって取り出しておき、FEREC の管理ページから行います。FEREC でのリストアについては、「FEREC520/720 取扱説明書」を参照して下さい。

- 手順 1: ［一括バックアップ取得］画面を開く

  Center2 管理ページより［FEREC 管理］→［一括バックアップ取得］画面を開きます。

- 手順 2: グループの選択

  ［グループ］のプルダウンメニューから、バックアップを取得するグループを選択します。

- 手順 3: バックアップ対象の選択

  ［バックアップ］プルダウンメニューでバックアップ対象を選択します。「すべて」、「設定のみ」または「カスタムページのコンテンツのみ」から選択できますが、通常は、「すべて（推奨）」を選択してください。

- 手順 4: バックアップ取得

 ［実行］ボタンを押すと、グループに属する全 FEREC のバックアップを取得します。

7.7. 一括ファームウェア更新

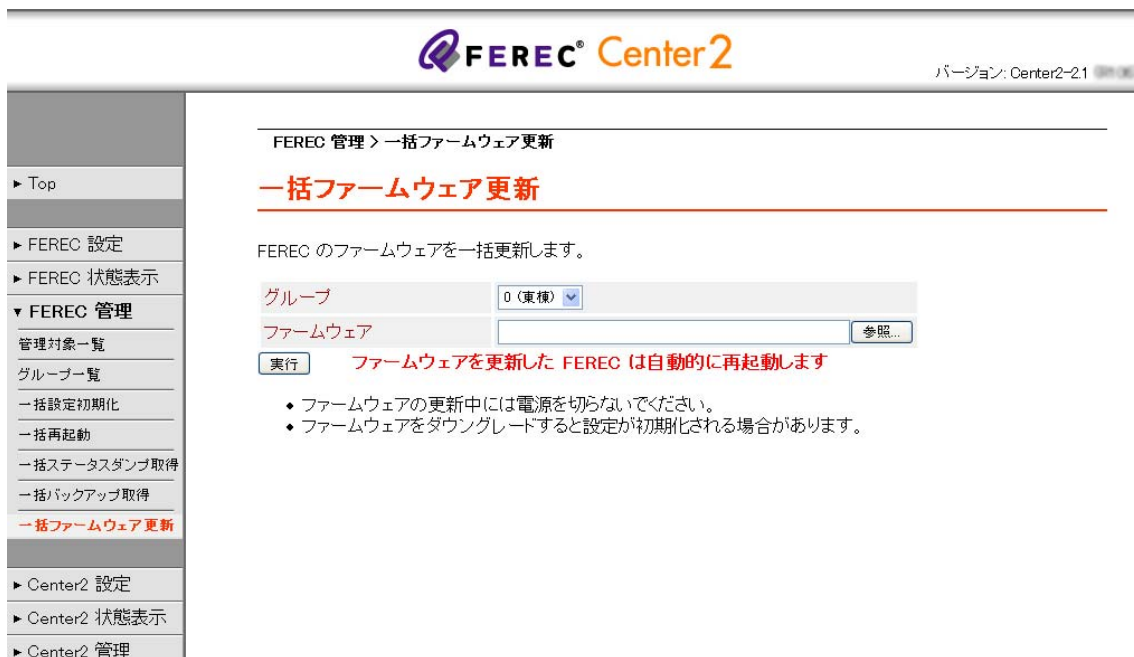
一括ファームウェア更新では、グループ登録した FEREC のファームウェアを一括して更新することができます。

なお、ファームウェアの更新中には Center2 および対象 FEREC の電源を切らないでください。また、ファームウェアをダウングレードした場合は、FEREC の設定が初期化される事があります。

- 手順 1：ファームウェアのダウンロード

  FERECのファームウェアを http://www.ferec.jp/ より管理用PCにダウンロードしてください。

- 手順 2: ［一括ファームウェア更新］画面を開く

  Center2 管理ページより［FEREC 管理］→［一括ファームウェア更新］画面を開きます。

- 手順 3: グループの選択

  ［グループ］のプルダウンメニューから、更新するグループを選択します。

- **手順 4: ファームウェアファイルを選択**

  直接入力または、［参照］ボタンを押して、ダウンロードしておいた FEREC ファームウェアファイルを選択します。

- **手順 5: ファームウェア更新**

  ［実行］ボタンを押すと、FEREC のファームウェアが更新され、FEREC は自動的に再起動します。

- **手順 6: ファームウェアバージョンの確認**

  FEREC の再起動が完了したら、再び Center2 管理ページより［FEREC 状態表示］→［FEREC 状態一覧］画面を開き、ファームウェアのバージョンが更新したバージョンであることを確認してください。

8. Center2 設定

Center2 設定には、以下の機能があります。

機能	概要
ネットワーク	Center2 のネットワークについて設定します。
システム設定	上記以外のシステム設定を行います。

FEREC® Center2
バージョン: Center2-2.1

▸ Top
▸ FEREC 設定
▸ FEREC 状態表示
▸ FEREC 管理
▾ Center2 設定
ネットワーク
システム設定
▸ Center2 状態表示
▸ Center2 管理

Center2 設定

Center2 設定

ネットワーク　Center2 のネットワークについて設定します。

システム設定　上記以外のシステム設定を行います。

8.1. ネットワーク

ネットワークには、以下の機能があります。

機能	概要
アドレス設定	Center2 の IP アドレス等を設定します。
DNS 設定	DNS の設定を行います。

8.1.1. アドレス設定

アドレス設定では、Center2 の IP アドレスおよびデフォルトルートを設定します。

- **手順 1：［アドレス設定］画面を開く**

　Center2 管理ページより［Center2 設定］→［ネットワーク］→［アドレス設定］画面を開きます。

- **手順 2：IP アドレスの設定**

　［IP アドレス］欄に Center2 の IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。また、ネットマスク長をプルダウンメニューから選択します。

- **手順 3: デフォルトルートの設定（任意）**

　Center2 のデフォルトルートを設定します。［デフォルトルート］欄にデフォルトゲートウェイの IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

- **手順 4: 設定**

　［設定］ボタンを押すと記入した内容で設定し、Center2 は自動的に再起動します。

8.1.2. DNS 設定

DNS 設定では、Center2 が利用する DNS サーバを設定します。DNS サーバは、IP アドレスで指定します。

なお、DNS サーバは、最大 2 台まで設定できます。

- 手順 1：［DNS 設定］画面を開く

 Center2 管理ページより［Center2 設定］→［ネットワーク］→［DNS 設定］画面を開きます。

- 手順 2：IP アドレスの設定

 DNS サーバの IP アドレスを設定します。［DNS サーバ 1］欄および［DNS サーバ 2］欄に IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

- 手順 3: 設定

 ［設定］ボタンを押すと指定した DNS サーバが設定されます。

8.2.　システム設定

システム設定には、以下の機能があります。

機能	概要
管理許可アドレス設定	管理許可アドレスの設定を行います。
HTTPS 設定	HTTPS 接続の設定を行います。
syslog 設定	ログを転送する syslog サーバの設定を行います。
時刻設定	内部時計の設定、NTP サーバの設定を行います。

FEREC Center2　バージョン: Center2-2.1

▸ Top
▸ FEREC 設定
▸ FEREC 状態表示
▸ FEREC 管理
▾ Center2 設定
ネットワーク
システム設定
管理許可アドレス設定
HTTPS 設定
syslog設定
時刻設定
▸ Center2 状態表示
▸ Center2 管理

Center2 設定 > システム設定

システム設定

管理許可アドレス設定　管理許可アドレスの設定を行います。

HTTPS 設定　HTTPS 接続の設定を行います。

syslog設定　ログを転送する syslog サーバの設定を行います。

時刻設定　内部時計の設定、NTP サーバの設定を行います。

8.2.1. 管理許可アドレス設定

Center2 では、管理ページおよび管理コンソール（telnet,ssh）を、許可した特定のアドレスのみに制限することができます。

管理許可アドレス設定では、許可するアドレスを、最大 5 個まで登録できます。

なお、MNT ポートにはこの管理許可アドレスによる制限は適用されず、常に接続できます。

また、工場出荷時は、制限していません。

管理許可アドレスを追加する場合

- 手順 1：［管理許可アドレス設定］画面を開く

  Center2 管理ページより［Center2 設定］→［システム設定］→［管理許可アドレス設定］画面を開きます。

- **手順 2: アドレスの入力画面を開く**

  ［新しい管理許可アドレスの追加］ボタンを押して、アドレスの入力画面を開きます。

FEREC® Center2
バージョン: Center2-2.1

▸ Top
▸ FEREC 設定
▸ FEREC 状態表示
▸ FEREC 管理
▾ Center2 設定
ネットワーク
システム設定
管理許可アドレス設定
HTTPS 設定
syslog設定
時刻設定
▸ Center2 状態表示
▸ Center2 管理

Center2 設定 > システム設定 > 管理許可アドレス設定

管理許可アドレス設定

管理許可アドレス ／ 0
設定

- 管理ページ、管理コンソール（telnet, ssh）に接続できるアドレスを指定します。
- 管理許可アドレスは最大 5 個まで追加可能です。
- ネットワーク全体を指定する場合 192.168.15.0/24 のように CIDR 表記で指定します。
- 単一のホストを指定する場合 192.168.15.10/32 のようにネットマスク長を 32 にします。
- MNT ポートにはこの管理許可アドレスによる制限は適用されず、常に接続できます。

- **手順 3: 管理許可アドレスの入力**

  ［管理許可アドレス］欄に登録する IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。また、ネットマスク長をプルダウンメニューから選択します。管理許可アドレスはネットワークまたは単一ホストで指定します。ネットワーク全体を指定する場合は 192.168.15.0/24 のように CIDR 表記で指定します。単一のホストを指定する場合は 192.168.15.10/32 のようにネットマスク長を 32 にします。

- **手順 4: 設定**

  ［設定］ボタンを押すと管理許可アドレスが追加されます。

管理許可アドレスを削除する場合

- 手順 1：［管理許可アドレス設定］画面を開く

　Center2 管理ページより［Center2 設定］→［システム設定］→［管理許可アドレス設定］画面を開きます。

- 手順 2: 管理許可アドレスの削除

　管理許可アドレスの右横にある［削除］ボタンを押すと、該当のアドレスが管理許可アドレスから削除されます。

8.2.2. HTTPS 設定

Center2 では、管理ページへのアクセスに HTTPS を使用することができます。

HTTPS設定では、管理ページへのアクセスにHTTPまたはHTTPSどちらを使用するか設定します。HTTPSを使用する場合は、先に“8.2.2.1. 証明書インポート”を行ってください。

なお、MNT ポートは、HTTPS 設定の設定内容にかかわらず、常に HTTP のみで接続できます。

- 手順 1：［HTTPS 設定］画面を開く

  Center2 管理ページより［Center2 設定］→［システム設定］→［HTTPS 設定］画面を開きます。

- 手順 2: 接続プロトコルの選択

  ［接続プロトコル］のプルダウンメニューから、管理ページへのアクセスに使用するプロトコルとして「HTTP」または「HTTPS」どちらかを選択します。

- 手順 3: 設定

  ［設定］ボタンを押すと、管理ページへのアクセスに使用するプロトコルが設定され、自動的に再起動します。

8.2.2.1.　証明書インポート

証明書インポートでは、HTTPS で使用する証明書及び鍵ファイルをインポートします。必要な場合は、中間 CA 証明書も使用できます。

各証明書および鍵ファイルは PEM 形式のみ使用できます。但し、パスフレーズの設定された鍵ファイルは使用できません。また、使用できる証明書および鍵ファイルはいずれも 4KB 以内です。

各証明書および鍵ファイルがすでにインポートしてある場合、再びインポートを行うと以前の証明書および鍵ファイルを上書きします。

- **手順 1：［証明書インポート］画面を開く**

  Center2 管理ページより［Center2 設定］→［システム設定］→［HTTPS 設定］→［証明書インポート］画面を開きます。

- **手順 2: サーバ証明書ファイル名の設定**

  ［サーバ証明書ファイル］欄に直接、または、［参照］ボタンを押して、サーバ証明書ファイルのファイル名を設定します。

- 手順 3: 鍵ファイル名の設定

　［鍵ファイル］欄に直接、または、［参照］ボタンを押して、鍵ファイルのファイル名を設定します。

- 手順 4: 中間 CA 証明書ファイル名の設定

　［中間 CA 証明書ファイル］欄に直接、または、［参照］ボタンを押して、中間 CA 証明書ファイルのファイル名を設定します。

　中間 CA 証明書が不要な場合はファイル名を省略します。

- 手順 5: インポート

　［インポート］ボタンを押すと、ファイル名を設定した各ファイルを Center2 にインポートします。

8.2.2.2. 証明書エクスポート

証明書エクスポートでは、Center2 本体にインポート済みの証明書ファイルを取り出すことができます。

証明書のエクスポートは、以下の手順で行います。

- 手順 1：［証明書エクスポート］画面を開く

  Center2 管理ページより［Center2 設定］→［システム設定］→［HTTPS 設定］→［証明書エクスポート］画面を開きます。

- 手順 2: エクスポート

  各ファイル名の右にある［エクスポート］ボタンを押すと、それぞれのファイルが管理用 PC に保存できます。

8.2.3. syslog 設定

Center2 では、Center2 自身のログを外部の syslog サーバに送信することができます。syslog 設定では、syslog サーバを設定します。

なお、FEREC のログを syslog サーバに送信する場合は、FEREC 個々に設定する必要があります。管理対象 FEREC のログを Center2 経由で syslog サーバへ転送することはできません。

- 手順 1：［syslog 設定］画面を開く

  Center2 管理ページより［Center2 設定］→［システム設定］→［syslog 設定］画面を開きます。

FEREC Center2
バージョン: Center2-2.1
Top
FEREC 設定
FEREC 状態表示
FEREC 管理
Center2 設定
ネットワーク
システム設定
管理許可アドレス設定
HTTPS 設定
syslog設定
時刻設定
Center2 状態表示
Center2 管理
Center2 設定 > システム設定 > syslog設定
syslog設定
サーバ名
ファシリティ local2
レベル NOTICE
設定
syslog サーバをホスト名か IP アドレスで指定します。

- 手順 2: サーバ名の設定

  ［サーバ名］欄に syslog サーバのホスト名または IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

- 手順 3: ファシリティの選択

  ［ファシリティ］のプルダウンメニューから syslog サーバへログを送信する際のファシリティを選択します。選択可能なファシリティは、「local0」～「local7」です。

- **手順 4: レベルの選択**

　［レベル］のプルダウンメニューから syslog サーバへ送信するレベルを選択します。
　Center2 は、重大度がここで選択したレベル以上のログを syslog サーバへ送信します。重大度は高い方から順に、「ERR」、「WARN」、「NOTICE」、「INFO」、「DEBUG」となります。

- **手順 5: 設定**

　［設定］ボタンを押すと syslog サーバが設定されます。

8.2.4. 時刻設定

時刻設定では、Center2 本体の時刻を設定します。設定方法は、NTP サーバ指定か直接設定かを選ぶことができます。

NTP サーバを指定する場合

- 手順 1：［時刻設定］画面を開く

  Center2 管理ページより［Center2 設定］→［システム設定］→［時刻設定］画面を開きます。

FEREC Center2
バージョン: Center2-2.1

▸ Top
▸ FEREC 設定
▸ FEREC 状態表示
▸ FEREC 管理
▾ Center2 設定
ネットワーク
システム設定
管理許可アドレス設定
HTTPS 設定
syslog設定
時刻設定
▸ Center2 状態表示
▸ Center2 管理

Center2 設定 > システム設定 > 時刻設定

時刻設定

NTP サーバ
直接設定 2008 年 1 月 1 日 0 時 0 分
設定

- NTP サーバを選択した場合は、NTP サーバもしくは SNTP サーバをホスト名か IP アドレスで指定します。
- 直接設定を選択した場合は、時刻を合わせて「設定」ボタンを押してください。秒は 00秒になります。
- 設定時刻は、2000年 1月 1日 0時 0分以降を指定してください。

- 手順 2: NTP サーバの選択

  ラジオボタンで NTP サーバを選択します。

- 手順 3: サーバの設定

  ［NTP サーバ］欄に NTP サーバもしくは SNTP サーバのホスト名または IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

- 手順 4: 設定

  ［設定］ボタンを押すと NTP サーバとの時刻同期を開始します。

時刻を直接設定する場合

● 手順 1： ［時刻設定］画面を開く

Center2 管理ページより［Center2 設定］→［システム設定］→［時刻設定］画面を開きます。

FEREC Center2
バージョン: Center2-2.1

▸ Top
▸ FEREC 設定
▸ FEREC 状態表示
▸ FEREC 管理
▾ Center2 設定
ネットワーク
システム設定
管理許可アドレス設定
HTTPS 設定
syslog設定
時刻設定
▸ Center2 状態表示
▸ Center2 管理

Center2 設定 > システム設定 > 時刻設定

時刻設定

NTP サーバ
直接設定 2008 年 1 月 1 日 0 時 0 分
設定

- NTP サーバを選択した場合は、NTP サーバもしくは SNTP サーバをホスト名か IP アドレスで指定します。
- 直接設定を選択した場合は、時刻を合わせて「設定」ボタンを押してください。秒は 00秒になります。
- 設定時刻は、 2000年 1月 1日 0時 0分以降を指定してください。

● 手順 2: 直接設定の選択

［直接設定］の左にあるラジオボタンを選択します。

● 手順 3: 時刻の設定

［年］、［月］、［日］、［時］、［分］欄に時刻を設定します。それぞれ前後に空白文字が入らないようにしてください。秒は 00 秒になります。

● 手順 4: 設定

［設定］ボタンを押すと、指定した時刻に設定します。

9. Center2 状態表示

Center2 状態表示には、以下の機能があります。

機能	概要
ログ	Center2 自身のログを表示します。
設定一覧	設定情報を一覧表示します。
本体情報	本体の情報を表示します。

FEREC Center2
バージョン: Center2-2.1

▸ Top
▸ FEREC 設定
▸ FEREC 状態表示
▸ FEREC 管理
▸ Center2 設定
▾ Center2 状態表示
ログ
設定一覧
本体情報
▸ Center2 管理

Center2 状態表示

Center2 状態表示

ログ Center2 自身のログを表示します。

設定一覧 設定情報を一覧表示します。

本体情報 本体の情報を表示します。

9.1. ログ

システムログは Center2 本体に関するログを、デバッグログは Center2 本体の保守に関するログを最大 10000 件まで表示できます。また、ログを管理用 PC にダウンロードできます。

ログは、外部のsyslogサーバを設定して、送信することもできます。syslogサーバの設定は、“8.2.3. syslog設定” を参照してください。

NOTE

- ダウンロードされるログは、表示されている内容をそのままダウンロードするのではなく、［ダウンロード］ボタンを押した時点の内容になります。

ログを表示する場合

- 手順 1：［ログ］画面を開く

Center2 管理ページより［Center2 状態表示］→［ログ］画面を開くと、ログが表示されます。

FEREC Center2
バージョン: Center2-2.1

Top
FEREC 設定
FEREC 状態表示
FEREC 管理
Center2 設定
Center2 状態表示
ログ
設定一覧
本体情報
Center2 管理

Center2 状態表示 > ログ

ログ

表示開始時刻 2008 年 9 月 25 日 12 時
表示終了時刻 2008 年 9 月 25 日 17 時
ログ種別 システムログ

表示 ダウンロード

2008-09-25 12:00:23 tund[3058]: connection closed <1>172.16.3.65
2008-09-25 12:00:27 tund[4509]: connection established <0>172.16.3.63
2008-09-25 12:00:53 tund[3894]: connection established <1>172.16.3.65

ログの表示条件を指定する場合

- **手順 1：［ログ］画面を開く**
  Center2 管理ページより［Center2 状態表示］→［ログ］画面を開きます。

- **手順 2: 表示条件の設定**
  以下の表示条件を設定することで、ログの表示内容を指定できます。

指定条件	内容
表示開始時刻	表示を開始する時刻を時単位で指定します。初期値は現在時刻（但し分以下を切り捨て）の 1 時間前です。
表示終了時刻	表示を終了する時刻を時単位で指定します。初期値は現在時刻（但し分以下を切り捨て）の 1 時間後です。
ログ種別	表示するログの種別を「システムログ」および「デバッグログ」から選択します。初期値は「システムログ」です。

- **手順 3: 表示**
  ［表示］ボタンを押すと、指定した条件でログが表示されます。

ログをダウンロードする場合

- **手順 1：［ログ］画面を開く**
  Center2 管理ページより［Center2 状態表示］→［ログ］画面を開きます。

- **手順 2: ダウンロード条件の設定**
  ログを表示する場合と同様に条件を設定することで、ダウンロードする内容を指定できます。

- **手順 3: ダウンロード**
  ［ダウンロード］ボタンを押すと、指定した条件でログをダウンロードできます。

9.2. 設定一覧

Center2 本体の設定内容を表示します。

- **手順 1：［設定一覧］画面を開く**

  Center2 管理ページより［Center2 状態表示］→［設定一覧］画面を開くと、Center2 本体の設定内容が表示されます。

FEREC Center2 バージョン: Center2-2.1

▸ Top
▸ FEREC 設定
▸ FEREC 状態表示
▸ FEREC 管理
▸ Center2 設定
▾ Center2 状態表示
ログ
設定一覧
本体情報
▸ Center2 管理

Center2 状態表示 > 設定一覧

設定一覧

```
# Center2 (FDJ0) configuration file
# firmware version: Center2-2.1
# serial number: FDJ-0000-0003
# last modified: 2008-09-25 09:39:55
network address 172.16.3.64/24
network default-route add 172.16.3.9
password admin "admin"
admin https disable
admin sshd disable
admin telnetd enable
syslog facility local2 notice
ntp disable
set prompt ""
```

9.3.　本体情報

Center2 本体に関する情報が表示されます。
表示されるのは、以下の項目です。

項目	内容
品名	Center2 と表示されます。
型番	Center2 の型番が表示されます。
シリアル番号	Center2 本体を一意に認識するための番号です。 弊社にお問い合わせ頂く際には、予めご確認ください。
ファームウェアのバージョン	現在動作しているファームウェアのバージョンです。 ファームウェアの更新を行った際、この内容で更新結果をご確認ください。
LAN MAC アドレス	LAN ポートの MAC アドレスです。
MNT MAC アドレス	MNT ポートの MAC アドレスです。

- 手順 1：［本体情報］画面を開く

　Center2 管理ページより［Center2 状態表示］→［本体情報］画面を開くと、Center2 本体に関する情報が表示されます。

FEREC Center2
バージョン: Center2-2.1
▸ Top
▸ FEREC 設定
▸ FEREC 状態表示
▸ FEREC 管理
▸ Center2 設定
▾ Center2 状態表示
ログ
設定一覧
本体情報
▸ Center2 管理
Center2 状態表示 > 本体情報
本体情報
品名 Center2
型番 FDJ400
シリアル番号 FDJ-0000-0003
ファームウェアのバージョン Center2-2.1
LAN MAC アドレス
MNT MAC アドレス

10. Center2 管理

Center2 管理には、以下の機能があります。

機能	概要
ディスク管理	データディスク(RAID)の状態表示、管理を行います。
パスワード	管理者パスワードの設定を行います。
初期化	設定またはログを初期化し、工場出荷時状態に戻します。
再起動	Center2 を再起動します。
停止	Center2 を停止し、電源を OFF にします。
ステータスダンプ	障害解析用のステータスダンプを取得します。
バックアップ	設定のバックアップ、リストアを行います。
ファームウェア更新	ファームウェアの更新を行います。
ping	ping を使用して接続確認を行います。

10.1. ディスク管理

データディスク(RAID)の状態表示、管理を行います。

- 手順 1：［ディスク管理］画面を開く

Center2 管理ページより［Center2 管理］→［ディスク管理］画面を開くと、データディスクに関する情報が表示されます。

FEREC Center2
バージョン: Center2-2.1
▸ Top
▸ FEREC 設定
▸ FEREC 状態表示
▸ FEREC 管理
▸ Center2 設定
▸ Center2 状態表示
▾ Center2 管理
ディスク管理
パスワード
初期化
再起動
停止
ステータスダンプ
バックアップ
ファームウェア更新
Center2 管理 > ディスク管理
ディスク管理

ディスク情報	使用量	0.0 GB (0.0 %)
	空き容量	292.5 GB
	総容量	292.5 GB
RAID 状態	DRIVE1	正常
	DRIVE2	正常

なお、表示されるのは、以下の項目です。

項目		内容
ディスク情報	使用量	データディスクの使用量が表示されます。
	空き容量	データディスクの空き容量が表示されます。
	総容量	データディスクの総容量が表示されます。
RAID 状態	DRIVE1	データディスクの RAID 状態が表示されます。表示される状態は、以下の別表のとおりです。
	DRIVE2	

また、表示される RAID 状態は、以下になります。

状態	説明
正常	正常に稼働中。
再構築中	再構築中。
異常(ディスク取り外し不可)	RAID として異常発生。
ディスクが接続されていません	本体にドライブが取り付けられていません。ドライブ取り付け後、disk attach コマンドの実行前もこの状態になります。
ディスクを接続してから再起動してください	ドライブを取り付けないまま Center2 が起動しています。Center2 を一旦停止してドライブを接続してから、再起動してください。

10.2. パスワード

管理者パスワードを設定します。管理者パスワードは、管理ページへアクセスおよび管理コンソールへログインする際に使用します。

- 手順 1：［パスワード］画面を開く
  Center2 管理ページより［Center2 管理］→［パスワード］画面を開きます。

- 手順 2：パスワードの入力
  ［管理者パスワード］欄に管理者パスワードを入力します。管理者パスワードは半角（ASCII コード 0x20～0x7e）3 文字以上 15 文字以下で記入します。

- 手順 3: 設定
  ［設定］ボタンを押すと、直ちに管理者パスワードが変更されます。

10.3. 初期化

Center2 の設定またはログを初期化します。設定を初期化すると、すべての設定が工場出荷時設定に戻ります。ネットワークアドレスも工場出荷時の値(192.168.45.1)に戻ります。ログを初期化すると、Center2 のログおよび管理対象 FEREC から受信したログおよびログイン履歴が削除されます。

- 手順 1：［初期化］画面を開く

  Center2 管理ページより［Center2 管理］→［初期化］画面を開きます。

- 手順 2: 初期化対象の選択

  ［初期化対象］のプルダウンメニューから、初期化対象を選択します。

- 手順 2: 初期化

  ［初期化］ボタンを押すと、初期化されます。「設定」または「すべて」を選択した場合は、自動的に再起動します。「ログ」を選択した場合は、再起動しませんが、ログ収集は停止します。ログ収集を再開する場合は、再起動が必要です。

10.4. 再起動

Center2 を再起動します。

- 手順 1：［再起動］画面を開く
  Center2 管理ページより［Center2 管理］→［再起動］画面を開きます。

- 手順 2: 再起動
  ［今すぐ再起動］ボタンを押すと、Center2 が再起動します。

10.5. 停止

Center2 を停止し、電源をオフにします。Center2 の電源を切る場合は、必ず、電源ボタンを押すか、この手順に従って停止を行ってください。

- 手順 1：［停止］画面を開く

  Center2 管理ページより［Center2 管理］→［停止］画面を開きます。

- 手順 2: 停止

  ［今すぐ停止］ボタンを押すと、Center2 が停止し、電源をオフにします。

10.6. ステータスダンプ

ステータスダンプでは、Center2 内部の情報をバイナリファイルとして、管理用 PC に保存できます。

Center2 に障害が発生した場合などに、ステータスダンプを弊社サポートセンターにご提供頂けますと、問題の早期解決につながることが期待できます。

- 手順 1：［ステータスダンプ］画面を開く

  Center2 管理ページより［Center2 管理］→［ステータスダンプ］画面を開きます。

- 手順 2: ステータスダンプ保存

  ［実行］ボタンを押すと、ステータスダンプを管理用 PC に保存します。

NOTE

- ステータスダンプには、再起動すると消えてしまう情報も多く含まれておりますので、Center2 の動作に問題が発生した場合は、再起動を試される前にステータスダンプを保存しておかれることをお勧めします。

10.7. バックアップ

バックアップでは、Center2 の設定内容を管理用 PC に保存できます。また、保存したバックアップファイルをリストアして、設定内容を復元できます。

NOTE

- FEREC ログ、FEREC ログイン履歴および Center2 本体のログは、バックアップでは保存されません。保存が必要な場合は、ダウンロードを使用して下さい。
- バックアップファイルはそのままリストアして下さい。例えば、一度解凍して再圧縮したような加工したバックアップファイルによるリストアは動作保証しておりません。

バックアップする場合

- 手順 1：［バックアップ］画面を開く

  Center2 管理ページより［Center2 管理］→［バックアップ］画面を開きます。

- **手順 2: バックアップ実行**

  ［バックアップ］下部の［実行］ボタンを押すと、バックアップファイルを管理用 PC に保存することができます。

リストアする場合

- **手順 1：［バックアップ］画面を開く**

  Center2 管理ページより［Center2 管理］→［バックアップ］画面を開きます。

- **手順 2: ファイル名の設定**

  ［リストア］欄に直接、または、［参照］ボタンを押して、バックアップファイルのファイル名を設定します。

- **手順 3: リストア実行**

  ［リストア］下部の［実行］ボタンを押すと、設定内容が復元され、Center2 は自動的に再起動します。

10.8. ファームウェア更新

Center2 は、常に最新のファームウェアでご利用頂く事をお勧めします。

Center2 のファームウェアを更新することにより、ご購入後に新たに追加・改良された機能をご利用いただくことができます。

なお、ファームウェアの更新中には電源を切らないでください。

また、ファームウェアをダウングレードした場合は、設定が初期化される事があります。

NOTE

- 以下の型番の Center2 は、対応バージョンより、低いバージョンにダウングレードする事は出来ません。

型番	対応バージョン
FDJ402	2.1.1 以上

- 手順 1：ファームウェアのダウンロード

Center2 のファームウェアを http://www.ferec.jp/ より管理用PCにダウンロードしてください。

- 手順 2: ［ファームウェア更新］画面を開く

Center2 管理ページより［Center2 管理］→［ファームウェア更新］画面を開きます。

FEREC Center2

バージョン: Center2-2.1

▸ Top
▸ FEREC 設定
▸ FEREC 状態表示
▸ FEREC 管理
▸ Center2 設定
▸ Center2 状態表示
▾ Center2 管理
ディスク管理
パスワード
初期化
再起動
停止
ステータスダンプ
バックアップ
ファームウェア更新

Center2 管理 > ファームウェア更新

ファームウェア更新

Center2 のファームウェアを更新します。
現在のファームウェアは です。

参照...
実行 自動的に再起動します

- ファームウェアの更新中には電源を切らないでください。
- ファームウェアをダウングレードすると設定が初期化される場合があります。

- **手順 3: ファームウェアファイルの選択**

  直接入力または、[参照] ボタンを押して、ダウンロードしておいたファームウェアファイルを選択します。

- **手順 4: ファームウェア更新**

  ［実行］ボタンを押すと、ファームウェアが更新され、Center2 は自動的に再起動します。

- **手順 5: ファームウェアバージョンの確認**

  再起動が完了したら、再び Center2 管理ページより［Center2 状態表示］→［本体情報］画面を開き、ファームウェアのバージョンが更新したバージョンであることを確認してください。

10.9. ping

ping では、Center2 から ping を行うことで、相手先との疎通を確認できます。

- 手順 1: ［ping］画面を開く

  Center2 管理ページより［Center2 管理］→［ping］画面を開きます。

- 手順 2: ホスト名または IP アドレスの入力

  ［ホスト名または IP アドレス］欄にホスト名または IP アドレスを半角で記入します。前後に空白文字が入らないようにしてください。

- 手順 3: ping 実行

  ［ping 実行］ボタンを押すと、ping を実行し、実行結果が表示されます。

NOTE

- ホスト名を使用する場合は、DNSサーバが設定されている必要があります。DNSサーバの設定方法は、“8.1.2. DNS設定”を参照してください。

11. CLI コマンド

11.1. CLI コマンド一覧

Center2 の CLI で使用可能なコマンドは以下になります。

CLI コマンド一覧

コマンド	頁
`admin https { enable | disable }`	139
`admin network add` *address/mask*	139
`admin network delete` *address/mask*	139
`admin sshd { enable | disable }`	139
`admin telnetd { enable | disable }`	140
`disk attach` *drive-id*	141
`disk detach` *drive-id*	142
`exit`	144
`group add` *group-id comment*	141
`group delete` *group-id*	141
`group node add` *group-id node-id*	141
`group node delete` *group-id node-id*	141
`halt`	144
`https-cert delete all`	141
`initialize { config | log | all }`	144
`logout`	144
`network address` *address/mask*	138
`network default-route add` *address*	138
`network default-route delete`	138
`network dns1 add` *address*	139
`network dns1 delete`	139
`network dns2 add` *address*	139
`network dns2 delete`	139
`node add` *node-id address version comment*	141
`node delete` *node-id*	141

（続く）

CLI コマンド一覧（続き）

コマンド	頁
ntp { enable | disable }	140
ntp server add *server*	140
ntp server delete	140
password admin *password*	139
ping *host*	144
raid initialize	142
remote group *group-id* account radius1 delete	149
remote group *group-id* account radius1 server *server*:*port* *secret* *timeout*	148
remote group *group-id* account radius2 delete	149
remote group *group-id* account radius2 server *server*:*port* *secret* *timeout*	148
remote group *group-id* admin network add *address*/*mask*	149
remote group *group-id* admin network delete *address*/*mask*	150
remote group *group-id* admin sshd { enable | disable }	150
remote group *group-id* admin telnetd { enable | disable }	150
remote group *group-id* auth guest add *username* *password* *comment* *policy-id*	148
remote group *group-id* auth guest delete *username*	148
remote group *group-id* auth ldap1 basedn *basedn*	147
remote group *group-id* auth ldap1 binddn *binddn* *bindpw*	146
remote group *group-id* auth ldap1 bindtype { direct | indirect }	146
remote group *group-id* auth ldap1 delete	148
remote group *group-id* auth ldap1 login-attribute *attribute*	147
remote group *group-id* auth ldap1 policy-attribute *attribute*	147
remote group *group-id* auth ldap1 server *uri* *policy-id* *timeout*	146
remote group *group-id* auth ldap1 version { 2 | 3 }	147
remote group *group-id* auth ldap2 basedn *basedn*	147
remote group *group-id* auth ldap2 binddn *binddn* *bindpw*	146
remote group *group-id* auth ldap2 bindtype { direct | indirect }	146
remote group *group-id* auth ldap2 delete	148
remote group *group-id* auth ldap2 login-attribute *attribute*	147
remote group *group-id* auth ldap2 policy-attribute *attribute*	147
remote group *group-id* auth ldap2 server *uri* *policy-id* *timeout*	146
remote group *group-id* auth ldap2 version { 2 | 3 }	147

（続く）

CLI コマンド一覧（続き）

コマンド	頁
remote group *group-id* auth order *auth1* [*auth2* [*auth3* [*auth4* [*auth5*]]]]	145
remote group *group-id* auth radius1 delete	145
remote group *group-id* auth radius1 server *server*:*port secret policy-id timeout*	145
remote group *group-id* auth radius1 with-macaddr delete	146
remote group *group-id* auth radius1 with-macaddr password *password*	145
remote group *group-id* auth radius2 delete	145
remote group *group-id* auth radius2 server *server*:*port secret policy-id timeout*	145
remote group *group-id* auth radius2 with-macaddr delete	146
remote group *group-id* auth radius2 with-macaddr password *password*	145
remote group *group-id* auth reject add *username*	148
remote group *group-id* auth reject delete *username*	148
remote group *group-id* client multiple-login { enable | disable }	150
remote group *group-id* client polling-interval *seconds*	150
remote group *group-id* client schedule { enable | disable }	150
remote group *group-id* client schedule open *hh*:*mm HH*:*MM*	151
remote group *group-id* html action *action-id* contents *filename*	152
remote group *group-id* html action *action-id* none	152
remote group *group-id* html action attach { enable | disable }	152
remote group *group-id* html action attach *actkey* { enable | disable }	152
remote group *group-id* html logo { enable | disable }	151
remote group *group-id* html message *msgkey* default	151
remote group *group-id* html message *msgkey message*	151
remote group *group-id* http-proxy { enable | disable }	156
remote group *group-id* http-proxy server add *address*:*port*	156
remote group *group-id* http-proxy server delete *address*:*port*	156
remote group *group-id* initialize	156
remote group *group-id* network dns1 add *address*	144
remote group *group-id* network dns1 delete	144
remote group *group-id* network dns2 add *address*	144
remote group *group-id* network dns2 delete	144
remote group *group-id* ntp { enable | disable }	153
remote group *group-id* ntp server add *server*	153

（続く）

CLI コマンド一覧（続き）

コマンド	頁
remote group *group-id* ntp server delete	154
remote group *group-id* password admin *password*	149
remote group *group-id* password webadmin *password*	149
remote group *group-id* policy add *policy-id name*	154
remote group *group-id* policy delete *policy-id*	154
remote group *group-id* policy ftp-proxy { enable | disable }	155
remote group *group-id* policy rule add *policy-id rule-id act dir proto address/mask* [*ports*]	154
remote group *group-id* policy rule delete *policy-id rule-id*	155
remote group *group-id* restart	156
remote group *group-id* set date *yyyy-mm-dd HH:MM*	156
remote group *group-id* syslog facility *facility level*	153
remote group *group-id* syslog server add *server*	153
remote group *group-id* syslog server delete	153
restart	144
set date *yyyy-mm-dd HH:MM*	143
set prompt *prompt*	143
show config	143
show config startup	143
show cpu	142
show disk	143
show https-cert	143
show interface	142
show log { system | debug }	143
show version	143
syslog facility *facility level*	140
syslog server add *server*	140
syslog server delete	140

11.2. CLI コマンド説明

Center2 の CLI で使用可能な各コマンドについて説明します。

なお、各コマンドの機能については、"5. FEREC設定"から"10. Center2 管理"もあわせてご覧下さい。

各コマンドについては、以下のように表記しています。

`show config`

タイプライターで示した文字はコマンドであることを示します。

val

イタリックで示した文字は変数であることを示します。

{ A | B | C | ... }

A、B、C、...のいずれかのうち1つを示します。

[*val***]**

val が省略可能であることを示します。

コマンドで指定する文字列が、空白や記号を含む場合は"（ダブルクォート）で文字列全体をクォートしてください。

`network address` *address/mask*

Center2 本体の IP アドレスおよびネットマスクを CIDR 表記で指定します。

設定は再起動後に有効になります。

`network default-route add` *address*

デフォルトゲートウェイを指定します。

設定は再起動後に有効になります。

`network default-route delete`

デフォルトゲートウェイの指定を削除します。

設定は再起動後に有効になります。

network dns1 add ***address***

network dns2 add ***address***

Center2 が利用する DNS サーバを設定します。DNS サーバは、IP アドレスで指定します。なお、DNS サーバは、最大 2 台まで設定できます。

設定は即有効になります。

network dns1 delete

network dns2 delete

DNS サーバの指定を削除します。

設定は即有効になります。

password admin ***password***

管理者パスワードを設定します。管理者パスワードは、管理ページへアクセスおよび管理コンソールへログインする際に使用します。

admin https { enable | disable }

管理ページへのアクセスに HTTPS を使用するか否かを指定します。

この指定に関係なく、MNT ポートからは常に HTTP でのみアクセス可能です。

設定は再起動後に有効になります。

admin network add ***address/mask***

管理ページおよび管理コンソール（telnet、ssh）へのアクセスを許可する管理許可アドレスを CIDR 表記で登録します。

設定は即有効になります。

admin network delete ***address/mask***

登録済みの管理許可アドレスを削除します。すべての管理許可アドレスを削除した場合、管理ページおよび管理コンソール（telnet、ssh）へのアクセス制限はなくなり、いずれのアドレスからもアクセス可能になります。

設定は即有効になります。

admin sshd { enable | disable }

管理コンソールへの ssh によるアクセスを許可するか否かを指定します。

この指定に関係なく、MNT ポートからは常に telnet でのみログイン可能です。

`admin telnetd { enable | disable }`

管理コンソールへの telnet によるアクセスを許可するか否かを指定します。

この指定に関係なく、MNT ポートからは常に telnet でログイン可能です。

`syslog facility` ***facility level***

syslog サーバへ送信するファシリティとレベルを指定します。

facility は、`local0`～`local7` の中から指定します。*level* は `err`、`warn`、`notice`、`info`、`debug` の中から指定し、指定したレベルとそれより重要度の高いログだけを送信します。

設定は syslog サーバが既に指定されていれば即有効に、syslog サーバが未指定ならば指定後有効になります。

`syslog server add` ***server***

Center2 が利用する syslog サーバを設定します。*server* に syslog サーバをホスト名か IP アドレスで指定します。なお、syslog サーバは、1 台のみ設定できます。

設定は即有効になります。

`syslog server delete`

syslog サーバの指定を削除します。

設定は即有効になります。

`ntp { enable | disable }`

Center2 本体の時刻を SNTP によって同期するかどうかを指定します。`enable` なら SNTP を用いて同期を行います。`disable` なら同期を行いません。

設定は即有効になります。

なお、Center2 はいずれの場合も NTP サーバにはなりません。

`ntp server add` ***server***

Center2 が利用する NTP サーバを設定します。*server* に SNTP サーバかあるいは NTP サーバをホスト名か IP アドレスで指定します。なお、サーバは、1 台のみ設定できます。

設定は即有効になります。

`ntp server delete`

NTP サーバの指定を削除します。

設定は即有効になります。

node add ***node-id address version comment***

管理対象の FEREC を登録します。*node-id* には登録するノード ID を 0～49 の中から、*address* は FEREC の IP アドレスを、*version* は 2 を、*comment* には登録する FEREC に関するコメントをそれぞれ指定します。

node delete ***node-id***

指定した FEREC を管理対象から削除します。*node-id* は削除したい FEREC のノード ID を指定します。

group add ***group-id comment***

グループを登録します。*group-id* はグループ ID を 0～31 の中から、*comment* には登録するグループに関するコメントをそれぞれ指定します。

group delete ***group-id***

グループを削除します。*group-id* は削除したいグループ ID を指定します。

group node add ***group-id node-id***

グループに FEREC を登録します。*group-id* は登録済みグループのグループ ID を、*node-id* には登録する FEREC のノード ID をそれぞれ指定します。なお、FEREC は、予め管理対象として登録しておく必要があります。

group node delete ***group-id node-id***

指定した FEREC をグループから削除します。*group-id* はグループ ID を、*node-id* は削除する FEREC のノード ID を指定します。

https-cert delete all

HTTPS で使用するためにインポートした証明書及び鍵ファイルを Center2 から削除します。

disk attach ***drive-id***

本体に接続済みで `failed` あるいは `not connected` な状態のドライブ を RAID に組み込み、再構築を行います。*drive-id* はドライブ番号で 1 か 2 を指定します。この操作を行ったドライブは `reconstructing` 状態になります。なお、再構築には、3～4 時間程度かかります。

ドライブの状態については、`show disk` コマンドを参照して下さい。

disk detach ***drive-id***

本体に接続中で optimal あるいは failed な状態のドライブを RAID から切り離し、not connected 状態にします。*drive-id* はドライブ番号で 1 か 2 を指定します。状態が not connected になれば本体からドライブを取り外すことができます。
ドライブの状態については、show disk コマンドを参照して下さい。

なお、以下の場合は detach できません。

- どちらかのドライブが reconstructing の場合、どちらも detach できません。
- 片方のドライブが optimal で、もう一方が optimal 以外の場合、optimal なドライブは detach できません。

NOTE

- ドライブの状態が not connected でない時にはドライブを取り外すことは出来ません。取り外した場合の動作は保証できません。
- Center2 を起動する際は、ドライブ 1、ドライブ 2 ともに必ず接続した状態で起動して下さい。

raid initialize

RAID の初期化を行います。RAID を初期化すると、Center2 ログ、FEREC ログおよび FEREC ログイン履歴は削除されます。初期化中は、FEREC との通信およびログ収集を停止します。初期化後、FEREC との通信およびログ収集を再開するには再起動してください。なお、初期化には、2～3 時間程度かかります。

show cpu

CPU の負荷状況とメモリの使用率を表示します。

show interface

ネットワークインタフェースの情報を表示します。

show disk

ディスクの情報を表示します。表示される状態とその内容は以下の通りです。

状態	説明
optimal	正常に稼働中。
reconstructing	再構築中。
failed	RAID として異常発生。
not connected	本体にドライブが取り付けられていません。ドライブ取り付け後、disk attach コマンドの実行前もこの状態になります。
not recognized	ドライブを取り付けないまま Center2 が起動しています。Center2 を一旦停止してドライブを接続してから、再起動してください。

show config

現在動作中の設定を表示します。

show config startup

次回起動時の設定を表示します。

show log { system | debug }

Center2 自身のログを表示します。

system はシステムログ、debug はデバッグログです。

show version

Center2 本体に関する情報を表示します。

show https-cert

Center2 自身の証明書および鍵ファイルに関する情報を表示します。

set date *yyyy-mm-dd HH:MM*

Center2 自身の時刻を設定します。秒は 00 秒になります。

set prompt *prompt*

CLI のプロンプトを *prompt* に設定します。15 文字以内です。

デフォルトは空です。

ping ***host***

ping を実行します。*host* はホスト名もしくは IP アドレスで指定します。

restart

Center2 を再起動します。

halt

Center2 を停止します。

initialize { config | log | all }

Center2 を初期化します。config を指定すると、設定を初期化し再起動します。設定を初期化すると、すべて工場出荷時の状態に戻ります。log を指定すると、ログを初期化してログ収集を停止しますが、再起動はしません。ログ収集を再開するには再起動してください。初期化するログには、Center2 ログ、FEREC ログおよび FEREC ログイン履歴が含まれます。all を指定すると、設定及びログを初期化し再起動します。

logout

CLI からログアウトします。

exit

CLI からログアウトします。

remote group ***group-id*** **network dns1 add** ***address***
remote group ***group-id*** **network dns2 add** ***address***

指定したグループに登録されている FEREC について、一括して DNS サーバを指定します。*group-id* はグループ ID を、*address* は IP アドレスを指定します。DNS サーバは FEREC 本体のホスト名の逆引き等に使用します。NAT/NAPT モードではクライアントに対して FEREC が DNS サーバになりますが、その際の上流 DNS サーバになります。なお、DNS サーバは、最大 2 台まで設定できます。
設定は即有効になります。

remote group ***group-id*** **network dns1 delete**
remote group ***group-id*** **network dns2 delete**

指定したグループに登録されている FEREC について、一括して DNS サーバの設定を削除します。*group-id* はグループ ID を指定します。
設定は即有効になります。

remote group *group-id* auth order *auth1* [*auth2* [*auth3* [*auth4* [*auth5*]]]]

指定したグループに登録されている FEREC について、一括して認証優先順位を決定します。*group-id* はグループ ID を、*auth1*～*auth5* は認証サーバを指定します。認証サーバは、guest、radius1、radius2、ldap1、ldap2 から指定します。

認証サーバは 1 つ以上 5 つまで記述できます。

但し、サーバが設定されていない RADIUS、LDAP サーバは、認証優先順位を設定していても認証時無視します。

設定は即有効になります。

remote group *group-id* auth radius1 server *server*:*port* *secret* *policy-id* *timeout*
remote group *group-id* auth radius2 server *server*:*port* *secret* *policy-id* *timeout*

指定したグループに登録されている FEREC について、一括して認証サーバ（RADIUS サーバ）を指定します。RADIUS サーバ設定は 2 セット持つことができるため radius1 または radius2 で指定します。

group-id はグループ ID を、*server* は RADIUS サーバのホスト名もしくは IP アドレスを、*port* はポート番号を指定します。標準のポート番号を使用する場合でも *port* を省略することはできません。

secret は RADIUS サーバの共有シークレットを、*policy-id* はこの認証サーバのデフォルトポリシー番号を、*timeout* はタイムアウト値を、秒単位で指定します。

remote group *group-id* auth radius1 delete
remote group *group-id* auth radius2 delete

指定したグループに登録されている FEREC について、一括して RADIUS サーバ 1 もしくは RADIUS サーバ 2 のすべての情報を削除します。*group-id* はグループ ID を指定します。

remote group *group-id* auth radius1 with-macaddr password *password*
remote group *group-id* auth radius2 with-macaddr password *password*

指定したグループに登録されている FEREC について、一括してクライアントの MAC アドレス認証を行うようにし、その際に使用するパスワードを設定します。*group-id* はグループ ID を、*password* はパスワードを 1 文字以上 127 文字以下で指定します。

設定は即有効になります。

remote group *group-id* auth radius1 with-macaddr delete
remote group *group-id* auth radius2 with-macaddr delete

指定したグループに登録されている FEREC について、一括して RADIUS サーバ 1 もしくは RADIUS サーバ 2 の MAC アドレス認証を行わないようにし、MAC アドレス認証用のパスワードを削除します。

group-id はグループ ID を指定します。

remote group *group-id* auth ldap1 server *uri policy-id timeout*
remote group *group-id* auth ldap2 server *uri policy-id timeout*

指定したグループに登録されている FEREC について、一括して認証サーバ（LDAP サーバ）を指定します。LDAP サーバ設定は 2 セット持つことができるため `ldap1` または `ldap2` で指定します。

group-id はグループ ID を指定します。

uri は *proto*`://`*server* `[:`*port*`]/`という書式で、*proto* は `ldap` もしくは `ldaps`、*server* には LDAP サーバのホスト名か IP アドレスが入ります。*port* はポート番号で省略可能です。省略した場合は標準ポート（LDAP なら 389、LDAPS なら 636）となります。

policy-id はこの認証サーバのデフォルトポリシー番号を、*timeout* はタイムアウト値を、秒単位で指定します。

設定は即有効になります。

remote group *group-id* auth ldap1 bindtype { direct | indirect }
remote group *group-id* auth ldap2 bindtype { direct | indirect }

指定したグループに登録されている FEREC について、一括して LDAP サーバのバインド方法を選択します。

group-id はグループ ID を指定します。

`indirect` は間接バインドであり、指定のバインド DN で一旦バインドした後、ベース DN 以下を検索する方式です。`direct` は直接バインドであり、ベース DN 直下の DN に直接バインドする方式です。通常は `indirect`（間接バインド）を使用します。

設定は即有効になります。

remote group *group-id* auth ldap1 binddn *binddn bindpw*
remote group *group-id* auth ldap2 binddn *binddn bindpw*

指定したグループに登録されている FEREC について、一括して LDAP サーバのバインド DN とバインドパスワードを指定します。

group-id はグループ ID を、*binddn* はバインド DN を、*bindpw* はバインドパスワードを指定します。

間接バインド方式の時のみ有効で、直接バインド時にはこの設定は無視します。
設定は即有効になります。

remote group *group-id* auth ldap1 basedn *basedn*
remote group *group-id* auth ldap2 basedn *basedn*

指定したグループに登録されている FEREC について、一括して LDAP サーバの検索ベース DN を指定します。
group-id はグループ ID を、*basedn* は検索ベース DN を指定します。
間接バインドでは検索ベース DN 以下を検索します。直接バインドでは検索ベース DN の直下を *login-attribute*=ユーザ名, *basedn* という DN でバインドします。
設定は即有効になります。

remote group *group-id* auth ldap1 login-attribute *attribute*
remote group *group-id* auth ldap2 login-attribute *attribute*

指定したグループに登録されている FEREC について、一括して LDAP サーバのユーザを検索する際の属性を指定します。
group-id はグループ ID を、*attribute* は属性を指定します。
設定は即有効になります。

remote group *group-id* auth ldap1 policy-attribute *attribute*
remote group *group-id* auth ldap2 policy-attribute *attribute*

指定したグループに登録されている FEREC について、一括して LDAP サーバのバインドした DN から、ポリシー名を取得する際の属性を指定します。省略した場合ポリシーはサーバのデフォルトが選択されます。
group-id はグループ ID を、*attribute* は属性を指定します。
設定は即有効になります。

remote group *group-id* auth ldap1 version { 2 | 3 }
remote group *group-id* auth ldap2 version { 2 | 3 }

指定したグループに登録されている FEREC について、一括して LDAP サーバの LDAP プロトコルのバージョンを指定します。*group-id* はグループ ID を指定します。初期状態ではバージョン 2 です。
設定は即有効になります。

remote group *group-id* auth ldap1 delete
remote group *group-id* auth ldap2 delete

指定したグループに登録されている FEREC について、一括して LDAP サーバ 1 もしくは LDAP サーバ 2 のすべての情報を削除します。*group-id* はグループ ID を指定します。

remote group *group-id* auth reject add *username*

指定したグループに登録されている FEREC について、一括して禁止アカウントの追加を行います。

group-id はグループ ID を、*username* は追加する利用を禁止するアカウントのアカウント名を指定します。

追加は即有効になります。

remote group *group-id* auth reject delete *username*

指定したグループに登録されている FEREC について、一括して禁止アカウントの削除を行います。

group-id はグループ ID を、*username* は削除する利用を禁止するアカウントのアカウント名を指定します。

削除は即有効になります。

remote group *group-id* auth guest add *username password comment policy-id*

指定したグループに登録されている FEREC について、一括して内部認証アカウントの追加を行います。

group-id はグループ ID を、*username* は追加するアカウントのアカウント名を、*password* はパスワードを、*comment* はコメントを、*policy-id* はポリシー番号を指定します。

ユーザ名、パスワード、コメントはいずれも 31 バイト以内で指定します。

remote group *group-id* auth guest delete *username*

指定したグループに登録されている FEREC について、一括して内部認証アカウントの削除を行います。

group-id はグループ ID を、*username* は削除するアカウントのアカウント名を指定します。

但し、このアカウント名で既にログイン中のユーザは影響を受けません。

remote group *group-id* account radius1 server *server*:*port secret timeout*
remote group *group-id* account radius2 server *server*:*port secret timeout*

指定したグループに登録されている FEREC について、一括して RADIUS アカウンティングサーバを指定します。

RADIUS アカウンティングサーバは設定は 2 セット持つことができるため、`radius1` または `radius2` で指定します。
group-id はグループ ID を、*server* は RADIUS アカウンティングサーバのホスト名もしくは IP アドレスを、*port* はポート番号を指定します。標準のポート番号を使用する場合でも *port* を省略することはできません。
secret は RADIUS アカウンティングサーバの共有シークレットを、*timeout* はタイムアウト値を、秒単位で指定します。

remote group *group-id* account radius1 delete
remote group *group-id* account radius2 delete

指定したグループに登録されている FEREC について、一括して RADIUS アカウンティングサーバ 1 もしくは RADIUS アカウンティングサーバ 2 のすべての情報を削除します。
group-id はグループ ID を指定します。

remote group *group-id* password webadmin *password*

指定したグループに登録されている FEREC について、一括してカスタムページ用の FTP パスワードを設定します。*group-id* はグループ ID を、*password* は設定するパスワードを指定します。初期値は `webadmin` です。
設定は即有効になります。

remote group *group-id* password admin *password*

指定したグループに登録されている FEREC について、一括して管理ページ GUI および CLI へのログインパスワードを設定します。*group-id* はグループ ID を、*password* は設定するパスワードを指定します。初期値は `admin` です。なお、ログインアカウント名は `admin` 固定です。
設定は即有効になります。

remote group *group-id* admin network add *address/mask*

指定したグループに登録されている FEREC について、一括して管理ページへ接続できるネットワークまたはホストを指定します。*group-id* はグループ ID を、*address* および *mask* は接続を許可するネットワークまたはホストを IP アドレス/ネットマスクで指定します。
アクセス制限は 5 つまで記述できます。何も記述しない場合はすべての接続を許可します。デフォルトはすべての接続を許可です。
アクセス制限は管理ページ、telnet や ssh による CLI、FTP 接続に適用されます。MNT

ポートからの接続にアクセス制限を適用することはできません。
設定は即有効になります。

remote group *group-id* admin network delete *address/mask*

指定したグループに登録されている FEREC について、一括して管理ページへ接続を許可しているネットワークまたはホストを削除します。*group-id* はグループ ID を、*address* および *mask* は接続許可を取り消す IP アドレス/ネットマスクを指定します。
設定は即有効になります。

remote group *group-id* admin sshd { enable | disable }

指定したグループに登録されている FEREC について、一括して CLI への ssh でのログインを許可するかどうかを指定します。
group-id はグループ ID を指定します。`enable` でログインを許可、`disable` で禁止します。
この設定に関わらずメンテナンスポートからは常に telnet でのみログイン可能です。

remote group *group-id* admin telnetd { enable | disable }

指定したグループに登録されている FEREC について、一括して CLI への telnet でのログインを許可するかどうかを指定します。
group-id はグループ ID を指定します。`enable` でログインを許可、`disable` で禁止します。
この設定に関わらずメンテナンスポートからは常に telnet でのみログイン可能です。

remote group *group-id* client polling-interval *seconds*

指定したグループに登録されている FEREC について、一括してクライアントの生存を確認するポーリング間隔を指定します。
group-id はグループ ID を、*seconds* はポーリング間隔を秒数で指定します。デフォルトは 120 秒です。

remote group *group-id* client multiple-login { enable | disable }

指定したグループに登録されている FEREC について、一括して重複ログインを許可するかどうかを指定します。
group-id はグループ ID を指定します。`enable` で重複ログインを許可、`disable` で禁止します。

remote group *group-id* client schedule { enable | disable }

指定したグループに登録されている FEREC について、一括して利用時間帯制限機能を

利用するかどうかを指定します。

group-id はグループ ID を指定します。`enable` で利用、`disable` で利用停止します。

remote group *group-id* client schedule open *hh*:*mm* *HH*:*MM*

指定したグループに登録されている FEREC について、一括して利用時間帯制限機能でユーザが FEREC を利用できる時間帯を指定します。

group-id はグループ ID を指定します。

24 時間表記で毎日 *hh:mm* から *HH:MM* まで利用できることを示します。*hh:mm* よりも *HH:MM* のほうが小さい場合は *hh:mm* から日をまたいで翌日の *HH:MM* まで利用可能であることを示します。

この設定は利用時間帯制限機能が利用可能である時のみ有効になります。

remote group *group-id* html logo { enable | disable }

指定したグループに登録されている FEREC について、一括してユーザ認証ページの認証フレーム中にある FEREC のロゴとバージョンを表示するかどうかを指定します。

group-id はグループ ID を指定します。`enable` で表示、`disable` で非表示にします。

remote group *group-id* html message *msgkey* default

remote group *group-id* html message *msgkey* *message*

指定したグループに登録されている FEREC について、一括してユーザ認証ページの認証フレーム中のメッセージを変更します。

group-id はグループ ID、*msgkey* はメッセージの識別子、*message* はメッセージを指定します。*message* の代わりに `default` を指定するとメッセージを初期状態に戻します。

変更可能なメッセージについては、“5.5.2. メッセージカタログ一括設定” を参照して下さい。

remote group *group-id* html action *action-id* none
remote group *group-id* html action *action-id* contents *filename*

指定したグループに登録されている FEREC について、一括して認証結果ごとの認証ページの動作を指定します。

group-id はグループ ID を指定します。

action-id は識別子で以下のいずれかを指定します。

action-id	説明
success	認証に成功した時
fail-passwd	ユーザ名かパスワードが原因で認証に失敗した時
fail-other	それ以外の原因で認証に失敗した時

動作が none なら何もアクションを起こしません。また動作が contents ならカスタムページ(右側のフレーム)を *filename* で指定されたページに変更します。*filename* はカスタムページのトップディレクトリにあるファイルのみ指定することができます。サブディレクトリにあるファイルや別のサーバにあるファイル(URL)を指定することは出来ません。

remote group *group-id* html action attach { enable | disable }

指定したグループに登録されている FEREC について、一括して、認証成功時の左フレームにクライアント情報を出力するかどうかを指定します。disable なら出力しません。enable なら以下のコマンドで出力するパラメータを指定します。

remote group *group-id* html action attach *actkey* { enable | disable }

指定したグループに登録されている FEREC について、一括して、認証成功時の左フレームに出力するクライアント情報を個別に指定します。この指定は各 FEREC が html action attach enable である場合のみ意味を持ちます。*actkey* は識別子で以下のいずれかを指定します。

actkey	説明
username	ログインしたユーザのユーザ名
policy-id	このクライアントに適用したポリシーの名前
policy-name	このクライアントに適用したポリシーの番号
mac-address	このクライアントの MAC アドレス(コロン区切り 16 進数形式)
hostname	FEREC の LAN 側ホスト名
wan-address	FEREC の WAN 側 IP アドレス(ドット区切り 10 進数形式)
location	FEREC の「場所名」
client-ip-address	このクライアントの IP アドレス(ドット区切り 10 進数形式)

`remote group` ***group-id*** **`syslog facility`** ***facility level***

指定したグループに登録されている FEREC について、一括して syslog サーバへ送信するファシリティとレベルを指定します。

group-id はグループ ID を指定します。*facility* は `local0`～`local7` の中からファシリティを指定します。*level* は `err`、`warn`、`notice`、`info`、`debug` の中からレベルを指定します。指定したレベルとそれより重要度の高いログだけを FEREC から syslog サーバへ送信します。

設定は syslog サーバが指定されていれば、即有効になります。

`remote group` ***group-id*** **`syslog server add`** ***server***

指定したグループに登録されている FEREC について、一括して syslog サーバを指定します。

group-id はグループ ID を、*server* は syslog サーバをホスト名か IP アドレスで指定します。指定できる syslog サーバは 1 つだけです。このコマンドで syslog サーバが指定されている場合のみ syslog が送信されます。

設定は即有効になります。

`remote group` ***group-id*** **`syslog server delete`**

指定したグループに登録されている FEREC について、一括して syslog サーバの指定を削除します。

group-id はグループ ID を指定します。

設定は即有効になります。

`remote group` ***group-id*** **`ntp { enable | disable }`**

指定したグループに登録されている FEREC について、一括して SNTP による時刻同期を行うかどうかを指定します。*group-id* はグループ ID を指定します。`enable` なら SNTP による時刻同期を行い、`disable` なら行いません。

設定は即有効になります。

なお、FEREC はいずれの場合も NTP サーバにはなりません。

`remote group` ***group-id*** **`ntp server add`** ***server***

指定したグループに登録されている FEREC について、一括して FEREC が参照する SNTP サーバもしくは NTP サーバを指定します。

group-id はグループ ID を、*server* は SNTP サーバもしくは NTP サーバを、ホスト名もしくは IP アドレスで指定します。指定できるサーバは 1 つだけです。

設定は即有効になります。

remote group *group-id* ntp server delete

指定したグループに登録されている FEREC について、一括して NTP サーバの指定を削除します。

group-id はグループ ID を指定します。

設定は即有効になります。

remote group *group-id* policy add *policy-id* *name*

指定したグループに登録されている FEREC について、一括してポリシー番号 *policy-id* のポリシーを追加します。*group-id* はグループ ID を、*name* はポリシー名を指定します。すでにポリシーが存在していれば名前の更新となります。

remote group *group-id* policy delete *policy-id*

指定したグループに登録されている FEREC について、一括してポリシー番号 *policy-id* のポリシーを削除します。*group-id* はグループ ID を指定します。

RADIUS および LDAP サーバのデフォルトポリシー、内部認証アカウント、スタティック NAT、スタティックブリッジのいずれかから参照しているポリシーは削除することができません。またポリシー0 およびポリシー1 を削除することは出来ません(内容を編集することはできます)。

remote group *group-id* policy rule add *policy-id* *rule-id* *act* *dir* *proto* *address/mask* [*ports*]

指定したグループに登録されている FEREC について、一括してポリシー番号 *policy-id* のルール番号 *rule-id* のポリシールールを定義します。*group-id* はグループ ID を指定します。ポリシー番号 *policy-id* は `policy add` コマンドにより定義されている必要があります。またルール番号 *rule-id* がすでに定義されている場合はルールの上書きになります。

act は動作で以下のいずれかを指定します。

act	説明
`pass`	パケットの通過を許可します。
`drop`	パケットの通過を禁止します。TCP に対しては TCP RST を返し、UDP, ICMP には ICMP Unreach を返します。
`pass-log`	`pass` と同じですが、同時にパケットログに出力します。
`drop-log`	`drop` と同じですが、同時にパケットログに出力します。

dir はルールの方向で以下のいずれかを指定します。

dir	説明
`in`	WAN 側から LAN 側方向
`out`	LAN 側から WAN 側方向

proto はプロトコル名もしくはプロトコル番号です。

proto	説明
`all`	すべてのプロトコル
`tcp`	TCP（6）
`udp`	UDP（17）
`gre`	GRE（47）

これ以外のプロトコルは数値（1～255）で指定します。但し IPv4 上のプロトコルでなければ制御できません。

address および *mask* はターゲットとなるアドレス範囲で、IP アドレスもしくは IP アドレスとネットマスクを CIDR 形式で指定します。`0.0.0.0/0` は `any` と記述することもできます。

ports はポート番号範囲の指定で、*proto* が TCP か UDP の場合のみ有効です。*ports* は単一のポート番号か、ポート番号の範囲指定が行えます。範囲指定の場合 “`21-23`” のように空白を入れずにハイフンで繋げて指定します。

`remote group` ***group-id*** **`policy rule delete`** ***policy-id rule-id***

指定したグループに登録されている FEREC について、一括してポリシールールを削除します。*group-id* はグループ ID を、*policy-id* はポリシー番号を、*rule-id* はルール番号を指定します。

`remote group` ***group-id*** **`policy ftp-proxy { enable | disable }`**

指定したグループに登録されている FEREC について、一括してアクセスコントロールの FTP プロキシ機能を有効にするかどうか指定します。*group-id* はグループ ID を指定します。

`enable` の場合、アクセスコントロールで TCP/21 を許可すると、FTP の制御セッションをプロキシしデータコネクションが通過できるように内部のフィルタの制御を自動的に行います。但しブリッジや NAT モードであっても FTP の制御セッションだけはクライアントの(WAN 側)アドレスからではなく FEREC 本体から張られることになります。これが問題になる環境では `disable` にしてください。一切 FTP プロキシを行わなくなります。

remote group *group-id* http-proxy { enable | disable }

指定したグループに登録されている FEREC について、一括して HTTP 外部プロキシ機能を有効にするかどうかを指定します。*group-id* はグループ ID を指定します。enable で有効に、disable で無効に設定します。、
設定は FEREC の再起動後に有効になります。

remote group *group-id* http-proxy server add *address*:*port*

指定したグループに登録されている FEREC について、一括して HTTP 外部プロキシ機能のためのプロキシサーバを指定します。*group-id* はグループ ID を、*address*:*port* はプロキシサーバの IP アドレスとポート番号を指定します。
プロキシサーバは５つまで指定できます。
設定は FEREC の再起動後に有効になります。

remote group *group-id* http-proxy server delete *address*:*port*

指定したグループに登録されている FEREC について、一括して HTTP 外部プロキシ機能のためのプロキシサーバの設定を削除します。*group-id* はグループ ID を、*address*:*port* は削除するプロキシサーバの IP アドレスとポート番号を指定します。
設定は FEREC の再起動後に有効になります。

remote group *group-id* set date *yyyy-mm-dd* *HH*:*MM*

指定したグループに登録されている FEREC について、一括して時刻を設定します。*group-id* はグループ ID を、*yyyy-mm-dd* は年月日を、*HH*:*MM* は時分を指定します。秒は 00 秒になります。

remote group *group-id* restart

指定したグループに登録されている FEREC を一括して再起動します。*group-id* はグループ ID を指定します。

remote group *group-id* initialize

指定したグループに登録されている FEREC を一括して工場出荷時の状態に初期化し、再起動します。*group-id* はグループ ID を指定します。
本コマンド実行後、引き続き FEREC を管理するためには、再度、各 FEREC で Center2 を設定する必要があります。

12. ハードウェア仕様

品名	Center2		
型番	FDJ402	FDJ401	FDJ400
外形寸法（幅×高さ×奥行)	426×43×574 mm (突起部含まず)		
重量	11.0kg	11.0kg	10.0kg
電源	AC100V　50/60Hz		
消費電力	150W	140W	160W
発熱量	540 [kJ/h]	504 [kJ/h]	576 [kJ/h]
動作環境	温度:10℃～35℃ 湿度:10%～90% (結露しないこと)		
イーサネットインタフェース	1 ポート（10/100/1000Base-T)		
メンテナンス用ポート	1 ポート（10/100/1000Base-T)		
シリアルポート	1 ポート（Dsub9 ピン　オス)		

13. 保証とアフターサービス

万一、保証期間中（保証書に記載されている期間）、製品の故障が発生した場合、ご購入の販売店、もしくは下記のサポートセンターまでご連絡ください。

保証期間中は、無償にてセンドバックによる修理をいたします。

■保証書（別添付）

保証書の規定に従って保守サービスを実施いたします。記載内容をお確かめの上、大切に保管してください。

■製品が故障したら・・・

（1）　ご購入の販売店、あるいはサポートセンターまでご連絡ください。

サポートセンターで症状を診断後、サポートセンターよりお客様に故障機器の送付をご依頼いたします（販売店から連絡させて頂く場合もございます）。

（2）　サポートセンターに故障機器をご送付ください。

機器の設定情報、データ等の保証及び復旧はいたしませんのでご了承ください。

送料はお客様にてご負担をお願いします。

お客様で製品に貼られたシール等、予めお剥がしの上ご送付下さい。製品の標準添付以外は一切の保護をいたしませんので予めご了承ください。

（3）　サポートセンターにて速やかに修理を行い、機器を返送いたします。

故障内容によっては、代替機との交換をもって修理とさせて頂く場合がございます。

■お問い合わせの前にご準備ください。

（1）　製品のシリアル番号をご確認ください（シリアル番号が不明な場合は、サポートを受けることはできません）。

（2）　障害内容をできるだけ詳細にご説明頂ける様ご準備ください。

（3）　保証書のご提示をお願いする場合がございます。

■保証期間を過ぎているときは・・・

修理によって機能が維持できる場合は、お客様のご要望により有償で修理をいたします。

■お問い合わせ窓口／機器送付先

Center2 に関するお問い合わせは、下記サポートセンターまでお願いいたします。

〒108-0073 東京都港区三田 3-12-16 山光ビル 2 階
（株）ネットスプリング　サポートセンター

TEL：050-5536-4841
URL：http://www.ferec.jp/
E-MAIL：nssc@netspring.co.jp

受付対応時間　月～金　9:00～17:00（祝祭日および年末年始 12/29～1/3 を除く）